BayRS Version 14.00

Part No. 308644-14.00 Rev 00
September 1999

4401 Great America Parkway
Santa Clara, CA 95054

Configuring SNMP, BootP, and DHCP Services

NORTEL NETWORKS™

Copyright © 1999 Nortel Networks

All rights reserved. Printed in the USA. September 1999.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks, AN, BN, and NetID are registered trademarks and ANH, ASN, BayRS, BayStack, BCC, and System 5000 are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible

for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xv
Text Conventions xvi
Acronyms xvii
Hard-Copy Technical Manuals xviii
How to Get Help xix

Chapter 1
Starting SNMP, BootP, and DHCP Services

Starting Configuration Tools 1-2
Configuring IP for Global Protocols 1-2
Step 1: Configuring a Physical Interface 1-2
Step 2: Configuring an IP Interface 1-3
Starting SNMP Services 1-5
Starting BootP Services 1-6
Starting BootP/DHCP Relay 1-7
Starting a DHCP Server 1-8

Chapter 2
SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts

SNMP Overview 2-2
SNMP Messages 2-2
SNMP Communities 2-4
SNMP Community Managers 2-4
SNMP View-Based Access Control 2-5
SNMP Implementation Notes 2-5
Internet Protocol 2-5
Events and Traps 2-5
Protocol Entities 2-6
Severity Levels 2-6

SNMP Trap Format 2-7
Thresholds 2-7
Threshold Example 2-8
Event Message Format 2-9
State of a Threshold 2-9
Memory Considerations 2-10
BootP Relay Agent Overview 2-10
DHCP Overview 2-14
Why Use DHCP? 2-14
Dynamic IP Address Allocation 2-15
DHCP Components 2-16
DHCP Clients 2-16
DHCP Server 2-16
NetID Server Manager 2-16
BootP/DHCP Relay Implementation 2-17
Acquiring an IP Address 2-18
Reacquiring the Same IP Address 2-22
DHCP Server Implementation 2-23
Acquiring an IP Address 2-24
Reacquiring the Same IP Address 2-27

Chapter 3
Customizing SNMP

Configuring SNMP Using the BCC and Site Manager 3-2
Customizing SNMP Global Parameters 3-3
Disabling and Reenabling SNMP 3-3
Enabling and Disabling the SNMP Lock Mechanism 3-4
Specifying a Lock Address 3-6
Specifying a Lock Timeout Value 3-6
Enabling and Disabling Authentication Failure Traps 3-7
Specifying the Type of Service for SNMP Packets 3-9
Adding SNMP Communities 3-9
Specifying an SNMP Community Name 3-9
Specifying Community Access Privileges 3-10
Deleting an SNMP Community 3-12

Configuring SNMP Community Managers 3-13
Adding a Manager 3-13
Configuring a Manager to Receive Traps 3-14
Specifying the Trap Port 3-14
Specifying a Trap Type 3-16
Deleting a Manager 3-17
Configuring SNMP View-Based Access Control 3-19
Configuring, Listing, and Deleting a View 3-19
Configuring a View 3-19
Listing All Views or the Contents of a View 3-21
Deleting a View or Its Contents 3-22
Configuring Communities and Their View Associations 3-22
Configuring a Community 3-23
Associating a View with a Community 3-23
Listing Community Information 3-23
Disassociating a View from a Community 3-24
Configuring Traps on the Router 3-25
Disabling a Trap Entity 3-27
Configuring Trap Exceptions 3-28
Deleting Trap Exceptions 3-30
Configuring Thresholds 3-31
Disabling and Reenabling Thresholds 3-31
Setting the Threshold Polling Interval 3-32
Adding a Threshold 3-33
Enabling and Disabling Thresholds for a Variable 3-33
Specifying a Value for the Threshold Level 3-34
Specifying the Severity Level for Event Messages 3-35
Specifying Threshold Units 3-36
Determining When to Record Threshold Events 3-37
Specifying the Maximum Number of Successive Alarms 3-37
Specifying Polling Intervals for Held Variables 3-38
Specifying a Threshold Object Name 3-39

Chapter 4
Customizing BootP

Customizing BootP Relay Agent Parameters 4-2
Disabling and Reenabling BootP 4-2
Enabling ARP Cache Support 4-3
Specifying the Maximum Number of Hops from Client to Server 4-4
Specifying a Minimum Timeout Value 4-5
Specifying the Relay Mode for Packet Forwarding 4-6
Setting Up the Routing Path from the BootP Server to the Router 4-7
Enabling BootP on Router Interfaces 4-7
Specifying Interfaces to Receive and Relay BOOTREQUEST Packets 4-9
Creating a BootP Relay Agent Forwarding Table 4-10
Specifying the IP Interface Input/Output Address Pair 4-10
Deleting an IP Interface Input/Output Address Pair 4-11
Disabling BootP Route Forwarding 4-12
Configuring an AN to Use EZ-Install over a Frame Relay PVC 4-13
Creating a BootP Client Interface Table 4-13
Specifying Servers for BootP Services 4-14
Configuring BootP Preferred Servers 4-15
Specifying the Target Server's Host Name 4-16
Disabling the Forwarding Route 4-16
Filtering BootP and DHCP Packets 4-17
Deleting the BootP Relay Agent from an IP Interface 4-18
Deleting BootP Globally 4-19

Chapter 5
Customizing BootP/DHCP Relay

Setting Up the Routing Path from the DHCP Server to the Router 5-2
Specifying Interfaces to Receive and Forward DHCP Packets 5-2
Defining DHCP Servers 5-3
Deleting BootP/DHCP Relay from an IP Interface 5-4
Deleting BootP/DHCP Relay Globally 5-5

Chapter 6
Customizing the DHCP Server

Modifying the DHCP Server Configuration 6-2
Configuring the NetID Server Manager IP Address 6-2
Specifying the DHCP Server IP Address 6-2
Specifying the DHCP Server TCP Port Number 6-3
Configuring the Number of Pings and the Ping Timeout 6-4
Specifying the DHCP Server Operating Mode 6-5
Specifying the Maximum Number of Pending Leases 6-6
Specifying the Debug Level 6-7
Disabling and Reenabling the DHCP Server 6-8
Deleting the DHCP Server from the Router 6-9
Deleting DHCP Globally 6-9

Appendix A
Site Manager Parameter Descriptions

SNMP Global Parameters A-3
SNMP Community Parameters A-5
SNMP Manager Parameters A-6
SNMP Trap Exception Parameters A-7
SNMP Threshold Global Parameters A-8
SNMP Threshold Interface Parameters A-9
BootP and DHCP Parameters A-16
BootP Relay Agent Interface Parameters A-16
BootP Address Parameters A-19
BootP Client Interface Address Parameters A-21
BootP Preferred Server Configuration Parameters A-22
DHCP Server Global Parameters A-24

Appendix B
SNMP show Commands

show snmp community B-2
show snmp stats B-3
show snmp trap-entity B-4
show snmp trap-event B-5

Index

Figures

Figure 2-1. Role of SNMP 2-3
Figure 2-2. BootP Client and Server on the Same Physical Network 2-10
Figure 2-3. BootP Client and Server on Different Physical Networks 2-11
Figure 2-4. BOOTREQUEST and BOOTREPLY Fields 2-12
Figure 2-5. BootP/DHCP Relay Implementation 2-17
Figure 2-6. Identifying DHCP Servers (BootP Relay Agent) 2-18
Figure 2-7. Requesting and Receiving IP Information (BootP Relay Agent) 2-21
Figure 2-8. DHCP Server Implementation 2-23
Figure 2-9. Identifying Routers Configured As DHCP Servers 2-24
Figure 2-10. Requesting and Receiving IP Information (DHCP Server) 2-26
Figure 4-1. Enabling BootP in a Sample Network 4-8

Tables

Table 2-1. Severity Levels 2-6
Table 2-2. Example of Threshold and Severity Settings 2-8
Table 2-3. IP Address Types Allocated by DHCP 2-15
Table 2-4. Fields in a DHCP Packet 2-19
Table 3-1. SNMP Configuration Tasks 3-2
Table 3-2. Trap Types Sent by the SNMP Agent 3-16

Preface

This guide describes Simple Network Management Protocol (SNMP), Bootstrap Protocol (BootP), BootP/Dynamic Host Configuration Protocol (DHCP) relay, and DHCP server and what you need to do to start and customize them on a Nortel Networks™ router.

You can use the Bay Command Console (BCC™) or Site Manager to configure these services on a router. In this guide, you will find instructions for using both the BCC and Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] **. . .** , you enter **ethernet/2/1** and as many parameter-value pairs as needed.

italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
ASN.1	abstract syntax notation
BootP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MAC	media access control

MIB	management information base
PDU	protocol data unit
PPP	Point-to-Point Protocol
RMON	remote monitoring
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	wide area network

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Chapter 1
Starting SNMP, BootP, and DHCP Services

This chapter describes how to create a basic SNMP, BootP, and BootP/DHCP Chapter 1, “Starting SNMP, BootP, and DHCP Servicesrelay configuration by specifying values for required parameters only and accepting default values for all other parameters of these services.

Topic	Page
Starting Configuration Tools	1-2
Configuring IP for Global Protocols	1-2
Starting SNMP Services	1-5
Starting BootP Services	1-6
Starting BootP/DHCP Relay	1-7
Starting a DHCP Server	1-8

For background information about these protocols and how they work, see Chapter 2, “SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts.”

Starting Configuration Tools

Before configuring SNMP, BootP, and DHCP services, refer to the following user guides for instructions on how to start and use the Nortel Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC)	*Using the Bay Command Console (BCC)*
Site Manager	*Configuring and Managing Routers with Site Manager*

These guides also describe generically how to create and modify a device configuration.

Configuring IP for Global Protocols

SNMP, BootP, and DHCP services all use the Internet Protocol (IP) for message transport. Before you configure SNMP, BootP, and DHCP services using the BCC or Site Manager, you must first start IP on the router.

Using the BCC

To start IP on the router:

1. **Configure a physical interface on an available slot/connector.**
2. **Configure an IP interface on the physical interface.**

Step 1: Configuring a Physical Interface

To configure a physical interface on a slot and connector, navigate to the top-level box or stack prompt and enter:

<interface_type> **slot** *<slot_number>* [**module** *<module_number>*] **connector** *<connector_number>*

- *interface_type* is the name of a link or net module on the router.
- *slot_number* is the number of the slot on which the link or net module is located.

- *module_number* is the net module number (ASN™ and System 5000™ routers only).
- *connector_number* is the number of a connector on the link or net module.

For example, the following command configures an Ethernet interface on slot 1, connector 2:

```
box# ethernet slot 1 connector 2
ethernet/1/2#
```

Step 2: Configuring an IP Interface

To configure an IP interface on a physical interface, navigate to the prompt for the physical interface and enter:

ip address <*address*> **mask** <*mask*>

address and *mask* are a valid IP address and its associated subnet mask, expressed in either dotted-decimal notation or in bit notation.

For example, the following command configures IP interface 2.2.2.2/255.0.0.0 on an Ethernet physical interface on slot 1, connector 2:

```
ethernet/1/2# ip address 2.2.2.2 mask 255.0.0.0
ip/2.2.2.2/255.0.0.0#
```

An IP interface is now configured on the Ethernet interface with default values for all interface parameters. When you configure an IP interface, the BCC also configures IP globally on the router with default values for all IP global parameters.

You can customize IP by modifying IP global and interface parameters as described in *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Using Site Manager

Before you can select a protocol to run on the router, you must configure a circuit that the protocol can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services* and *Configuring Ethernet, FDDI, and Token Ring Services.*

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, select **IP**. Then click on **OK**. If you plan to add BootP or DHCP services, you can also select BootP.	The IP Configuration window opens.
2. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see *Configuring IP, ARP, RARP, RIP, and OSPF Services* for parameter descriptions.	
3. Click on **OK**.	Site Manager displays a window asking whether you want to enable TFTP on the router.
4. Click on **Yes** to enable TFTP. Otherwise, click on **No**.	You return to the Configuration Manager window.

Starting SNMP Services

You can use the BCC command-line interface or the Site Manager graphical user interface to start SNMP on the router, accepting default values for all parameters.

SNMP is globally enabled on the router by default when you install BayRS software. By default, the Quick-Start installation script (*install.bat*) creates a read/write SNMP community named "public" with a wildcard manager (0.0.0.0) that allows universal read/write access. You should restrict read-write access to the router as soon as possible by reconfiguring the security of this SNMP community. When you add SNMP with the BCC, access is defined by default as read-only.

If you decide to change some or all of the default values, refer to the instructions in Chapter 3, "Customizing SNMP."

Before you begin, verify that IP is configured on an interface, as described in "Configuring IP for Global Protocols" on page 1-2.

Using the BCC

To configure SNMP on the router with default settings, begin in configuration mode at the box or stack prompt:

1. **Configure SNMP.**

   ```
   box# snmp
   ```

2. **Display SNMP default settings.**

   ```
   snmp# info
       lock enabled
       lock-address 0.0.0.0
       lock-timeout 2
       authentication-traps enabled
       type-of-service reliability
       state enabled
   ```

Using Site Manager

To start SNMP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **IP.**	The IP menu opens.
3. Choose **SNMP.**	The SNMP menu opens.
4. Choose **Global.**	The Edit SNMP Global Parameters window opens.
5. Click on **OK**.	You return to the Configuration Manager window.

Starting BootP Services

Using Site Manager, you can start BootP using default values for all parameters. If you decide to change some or all of the default values, see Chapter 4, "Customizing BootP."

Before you begin, verify that IP is configured on an interface, as described in "Configuring IP for Global Protocols" on page 1-2. You can also enable IP and BootP on an interface simultaneously.

To enable BootP on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the link or net module connector.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Choose **BOOTP** and click on **OK**.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Choose **File**.	The File menu opens.
7. Choose **Exit**.	You return to the Configuration Manager window.

Starting BootP/DHCP Relay

Using Site Manager you can start BootP/DHCP relay using default values for all parameters. If you decide to change some or all of the default values, see Chapter 5, "Customizing BootP/DHCP Relay."

Before you begin, you must verify that IP is configured on an interface, as described in "Configuring IP for Global Protocols" on page 1-2. You can also enable IP, BootP, and BootP/DHCP on the router simultaneously.

To enable BootP/DHCP relay on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System repsonds**
1. Enable BootP on the interface. For instructions, see "Starting BootP Services" on page 1-6.	
2. Choose **Protocols.**	The Protocols menu opens.
3. Choose **IP**.	The IP menu opens.
4. Choose **BOOTP**.	The BOOTP menu opens.
5. Choose **Relay Agent Interface Table**.	The BootP Relay Agent Interface Table window opens.
6. Set the **Pass Through Mode** parameter to **DHCP** or to **BootP/DHCP**.	
7. Click on **Apply**.	
8. Edit the parameters in this window. For instructions, see "Customizing BootP Relay Agent Parameters" on page 4-2.	You return to the Configuration Manager window.

Starting a DHCP Server

You must use Site Manager to start a DHCP server.

Before you begin, you must do the following:

1. Verify that IP is configured on an interface, as described in "Configuring IP for Global Protocols" on page 1-2.
2. Configure TCP on the router. For instructions on how to configure TCP on a router, see *Configuring IP Utilities*.
3. Configure the NetID® Server Manager to communicate with the DHCP server.

   For the DHCP server to operate, you must first install the NetID Server Manager on a Windows NT® or UNIX workstation and configure it to communicate with the DHCP server. Typically, you install the NetID Server Manager on the same workstation as the one that contains the NetID database.

   Because the DHCP server uses the information in the NetID database to assign IP addresses and host configuration information, you need to set up your network configuration using the NetID Management Console before the DHCP server can operate correctly.

   Using the NetID Management Console, you configure a DHCP server and make IP addresses available for dynamic allocation. For more information about installing the NetID Server Manager and setting your network configuration using the NetID Management Console, see the *NetID System Administrator's Guide*.

To create and enable the DHCP server on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Create DHCP**.	

After you create and enable the DHCP server on the router, you must enable the DHCP server on an IP interface. By default, the DHCP server is disabled on an IP interface. To enable the DHCP server on an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Set the **DHCP Server Enable** parameter to **Enable.** Click on **Help** or see the parameter description on page A-18.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

For information about modifying DHCP server parameters, see Chapter 6, “Customizing the DHCP Server.”

Chapter 2
SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts

This chapter describes the concepts behind SNMP, BootP, BootP/DHCP relay, and DHCP server services and how Nortel Networks routers implement them. You can use this information to decide how to customize SNMP, BootP, BootP/DHCP relay, and DHCP server parameters for your system.

Topic	Page
SNMP Overview	2-2
SNMP Implementation Notes	2-5
BootP Relay Agent Overview	2-10
DHCP Overview	2-14

SNMP Overview

SNMP is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP *applications* (also called SNMP *managers*) and SNMP *agents*.

SNMP applications contain manager software that runs on a network management station (also known as an SNMP client), such as a PC or a workstation. The manager software implements the protocols used to exchange data with SNMP agents. SNMP applications issue queries to gather information about the status, configuration, and performance of external network devices, called *network elements* in SNMP terminology. Network elements contain an agent and perform the network management function that the network management stations request.

The Nortel Networks Site Manager software is an example of a network management station, and the Nortel Networks Backbone Node (BN®) router is an example of a network element.

The *SNMP agent* is a software entity that responds to information and action request messages (SNMP get and set requests) sent by a network management station (your Site Manager workstation). The messages exchanged between manager and router SNMP agents enable you to access and manage objects in an active or inactive (stored) management information base (MIB) on a router.

The agents also send unsolicited reports (called *traps*) back to the network management station when certain network activity occurs. An example of a trap is an overload condition as defined by the packet load's crossing some threshold. You use the management station to configure, monitor, and receive trap messages from other network devices configured as SNMP agents. The management station can get and set objects in the agents and can receive traps from the agents. The management station, therefore, has the capability to "manage" a number of agents.

SNMP Messages

SNMP managers and network elements communicate with each other by sending SNMP messages (Figure 2-1).

The management station issues three types of SNMP messages to retrieve single or multiple object variables:

- *GetRequest* messages
- *GetNextRequest* messages
- *SetRequest* messages

The agent acknowledges all three types of messages by passing a *GetResponse* message to the management application. In addition, an agent may issue a trap to the network management station to identify a condition, such as a threshold that exceeds a predefined value.

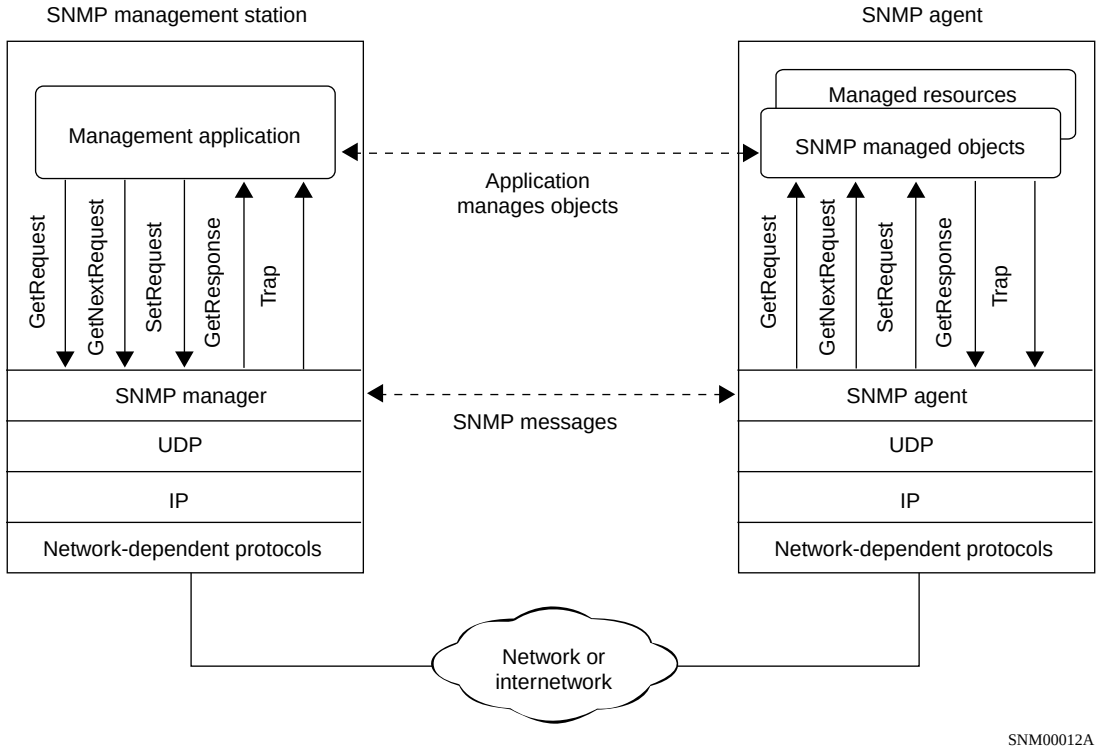

Figure 2-1. Role of SNMP

SNMP Communities

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request, by verifying that the manager belongs to a valid SNMP community. An *SNMP community* is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (within the agent), and all members of a community have the same access privileges, either read-only or read-write:

- *Read-only*: members can view configuration and performance information.
- *Read-write*: members can view configuration and performance information, and also change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

SNMP Community Managers

All SNMP message exchanges consist of a community name and a data field, which contains the SNMP operation and its associated operands. You can configure the SNMP agent to receive requests and send responses only from managers that are members of a known community.

If the agent knows the community name in the SNMP message and knows that the manager generating the request is a member of that community, it considers the message to be authentic and gives it the access allowed for members of that community. In this way, the SNMP community prevents unauthorized managers from viewing or changing the configuration of a router.

For information about configuring SNMP managers see “Configuring SNMP Community Managers” on page 3-13.

SNMP View-Based Access Control

SNMP *view-based access control* allows you to filter the information from an SNMP agent, thereby letting you control the view of the network. For example, a service provider can create a unique view for two different customers, so that each customer sees only the statistics and configuration information that the service provider wants each to see. The customer can view these statistics remotely using Site Manager.

To configure view-based access control, you must use either the BCC or the Technician Interface. You enable an SNMP *agent view* by associating a view with a community. A community can have only one agent view associated with it; however, the view itself can contain many different MIB subtree inclusions and exclusions.

For information about how to configure, list, or delete a view or its contents, see "Configuring SNMP View-Based Access Control" on page 3-19.

SNMP Implementation Notes

This section contains information about features specific to the Nortel Networks implementation of SNMP.

Internet Protocol

SNMP uses the User Datagram Protocol (UDP) to transport its messages. You must enable the Internet Protocol (IP) to use UDP and SNMP.

Events and Traps

An *event* is a change in the operating status of a router. The router stores the event as a single entry in a memory-resident log.

An *event log message* provides a brief description of an event, along with the event code associated with that event.

A *trap* is an event that the router transmits to the network management station.

SNMP allows you to configure which event log messages are sent to the network management station as traps. You select these traps based on slot, protocol entity, and severity level. You can also specify up to 50 *exceptions*, which are traps that the agent always sends, or never sends, regardless of slot and regardless of how you configure the trap parameters.

For information about how to specify which traps the agent sends, see "Configuring Traps on the Router" on page 3-25.

Protocol Entities

Events are always associated with a particular protocol entity. An *entity* is the software that generates a message. Entities include Nortel Networks software dedicated to the operation of a software service, such as Trivial File Transfer Protocol (TFTP) and IP, and the GAME operating system.

Both events and entities are assigned numeric codes. Together, this pair uniquely identifies a Nortel Networks router platform event. To access the event message database, look on the documentation CD that comes with BayRS or look on the Web at *support.baynetworks.com/library/tpubs/events*.

Severity Levels

Event and trap messages are always associated with a severity level. Table 2-1 describes the severity levels and gives the code that corresponds to each one. This guide does not cover Debug messages, because they are for Nortel Networks internal use only.

Table 2-1. Severity Levels

Severity	Description	Code
Information	Indicates routine events that usually require no action.	2
Warning	Indicates that a service acted in an unexpected manner.	4
Fault	Indicates a major service disruption, usually caused by a configuration, network, or hardware problem. The entities involved keep restarting until the problem is resolved.	8
Trace	Indicates information about each packet that traversed the network. Nortel Networks recommends viewing this type of trap message only when diagnosing network problems.	10
Debug	Indicates information that Nortel Networks Customer Support uses. These messages are not documented.	1

SNMP Trap Format

Some third-party network management applications, such as NetExpert, OpenView, and SunNet, let you trigger an operation when a specific SNMP trap is received. This section describes the SNMP trap format.

The router platform transmits a Nortel Networks event log trap as a 32-bit value as follows:

- Octets 1 and 2 (the most significant 16 bits) of the specific trap ID contain values of 1 and 0, respectively, to identify a Nortel Networks event log trap.
- Octet 3 of the specific trap ID contains a code that identifies the software entity that generated the trap.
- Octet 4 of the specific ID contains the event code that, in conjunction with the entity code, uniquely identifies the event.

Each 32-bit value is accompanied by three variable bindings that convey the event string that describes the trap condition, the slot that hosts the entity that generated the trap, and the trap severity (see Table 2-1).

Thresholds

SNMP uses a management information base (MIB) to manage the router. The MIB includes an extensive collection of statistics (MIB *variables*) that track the router's performance and provide early warnings of abnormal operating conditions.

With the Site Manager threshold feature, you can configure the agent to automatically notify you when specific statistics (or *instances* of the variable) reach certain levels.

You can set a threshold for any integer, counter, gauge, or time-tick variable in the MIB. Using the threshold parameters, you:

- Select the polling interval, which specifies how often the agent checks the statistic to see whether its value has reached the threshold.
- Set three threshold values (high, medium, and low).
- Specify the threshold action as *Lessthan* or *Greaterthan.*

For information about setting thresholds, see "Configuring Thresholds" on page 3-31.

When the statistic reaches the threshold, the agent generates an event. You specify the severity level at which you want the manager to log the event. Table 2-1 shows the available severity levels and their suggested meanings. Depending on how you configure the SNMP trap parameters (see “Configuring Traps on the Router” on page 3-25), the agent may also send the threshold exception as an SNMP trap.

The Site Manager threshold feature is functionally similar to the remote monitoring (RMON) Alarm and Event facility, with some minor differences. The Site Manager threshold feature provides three-tiered thresholds and defines a user-definable hysteresis mechanism. The RMON Alarm and Event facility provides a two-tiered proprietary threshold system. For information about RMON, RMON 2, and RMON alarms and events, see *Configuring RMON and RMON2*.

Threshold Example

Suppose you want SNMP to warn you if the number of high-priority (Priority Level 1) packets queued for transmission is approaching the maximum number supported by an interface. This maximum value is specified by the wfCctOptsCngcCfgQp1Threshold MIB object. Using the threshold parameters, you set a threshold for wfCctOptsCngcCfgQp1Threshold equal to 205.

You also set the polling interval to 20 seconds to indicate that, every 20 seconds, the agent should check variables for which you have configured thresholds. You set the threshold action to *Greaterthan* and set the threshold levels and severity of events to the values shown in Table 2-2.

Table 2-2. Example of Threshold and Severity Settings

Threshold Level	Low	Medium	High
Depth of Priority 1 transmit queue	102 (40% of capacity)	153 (60% of capacity)	205 (80% of capacity)
Severity of event	INFO	INFO	WARNING

When you add this threshold to the MIB, the agent polls the variable wfCctOptsCngcCfgQp1Threshold every 20 seconds and responds as follows:

- If its value is greater than 102, but less than or equal to 153, the manager logs an informational event indicating that the queue depth exceeded the low threshold.

- If its value is greater than 153 but less than or equal to 205, the manager logs an informational event indicating that the queue depth exceeded the medium threshold.
- If its value is greater than 205, the manager logs a warning event indicating that the queue depth exceeded the high threshold.

Event Message Format

By default, the threshold event messages include the MIB object identifier (OID) of the variable that exceeded the threshold, the value of the variable, and the threshold level exceeded.

For example, if the wfCctOptsCngcCfgQp1Threshold variable has a value of 120, the agent generates an event message similar to the following:

```
#1:08/27/99 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object 1.3.6.1.4.1.18.3.5.1.4.10.1.24 with value = 120 units/ hour
is > low threshold.
```

You can, however, identify objects more easily by configuring the software to report the object name rather than the OID in the event message. To configure the software to report the object name in the event message, use the Threshold Label parameter (see “Specifying a Threshold Object Name” on page 3-39).

For example, if you set the Threshold Label parameter to **wfCctOptsCngcCfgQp1Threshold**, the agent generates an event message similar to the following:

```
#1:08/27/99 10:53:20.802 INFO SLOT 2 STA CODE: 6
Object wfCctOptsCngcCfgQp1Threshold with value = 120 units/ hour is
> low threshold.
```

State of a Threshold

If the collision rate stays above a threshold for an extended period of time, the agent continues to generate a new event every 5 seconds. You can specify the maximum number of event messages that you want the agent to generate before it changes the threshold’s state to *held*.

When the threshold is in a held state, the agent does not generate new events unless the statistic exceeds the threshold at a different level. If the statistic does not exceed any threshold for a specified number of polling periods, the agent no longer considers the threshold held.

Memory Considerations

Polling statistics to determine whether they have reached a threshold and reporting events when variables exceed thresholds require router processing capacity. When you set many thresholds and use shorter polling intervals, the router performance will probably decline.

BootP Relay Agent Overview

BootP is built on the client-server model and allows a diskless client to boot remotely from a server on the same network or on a different physical network. The client broadcasts a request to boot from a remote server. When a suitable server receives the BOOTREQUEST packet, it responds to the client by issuing a BOOTREPLY packet, which includes the client's IP address, the address of the gateway, and the address of a server. The server then transmits the boot file to the client via a transfer protocol, such as Trivial File Transfer Protocol (TFTP).

Figure 2-2 illustrates how BootP works when the client and the server are on the same network. The client transmits a BOOTREQUEST packet to the IP broadcast address (255.255.255.255). The server sends a BOOTREPLY packet to the client. Depending on the server's implementation, the server addresses the packet to either the broadcast address or the client's IP address.

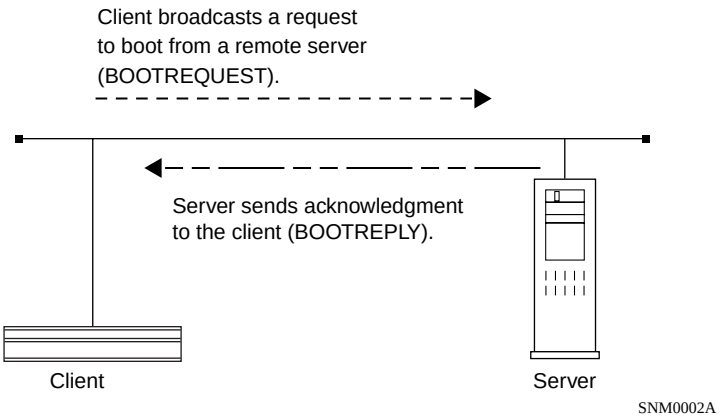

Figure 2-2. BootP Client and Server on the Same Physical Network

If, however, the client and the server are on different physical networks, a BootP *relay agent* (also known as a BootP *gateway*) must forward BootP packets to their correct destinations. When you configure a Nortel Networks router for BootP services, the router acts as a BootP relay agent. Figure 2-3 illustrates how BootP works when the client and the server are on different physical networks.

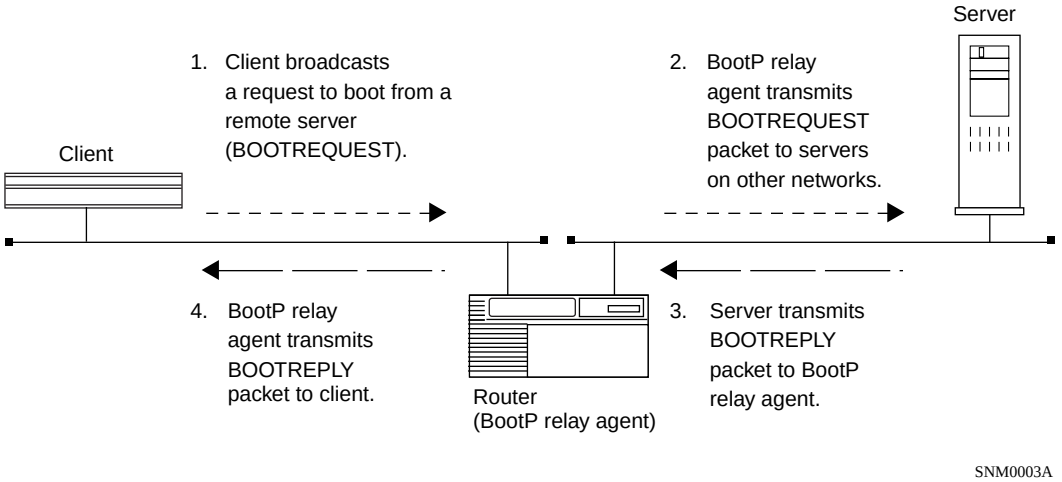
Server
1. Client broadcasts a request to boot from a remote server (BOOTREQUEST).
2. BootP relay agent transmits BOOTREQUEST packet to servers on other networks.
Client
4. BootP relay agent transmits BOOTREPLY packet to client.
3. Server transmits BOOTREPLY packet to BootP relay agent.
Router
(BootP relay agent)
SNM0003A

Figure 2-3. BootP Client and Server on Different Physical Networks

The client transmits a BOOTREQUEST packet to the IP broadcast address (255.255.255.255). The router receives the BOOTREQUEST packet at an interface that you configured to receive BOOTREQUEST packets (an input interface). If the BOOTREQUEST packet has an address other than 255.255.255.255, the router drops the packet.

Figure 2-4 shows the fields in the BOOTREQUEST and BOOTREPLY packets.

Operation (1)*	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction ID (4)			
Seconds (2)		Flags (2)	
Client IP address (4)			
Your IP address (4)			
Server IP address (4)			
Gateway IP address (16)			
Client hardware address (16)			
Server name (64)			
File name (128)			
Vendor-specific area (64)			
*The number in parentheses indicates the number of octets in each field.			

SNM0001A

Figure 2-4. BOOTREQUEST and BOOTREPLY Fields

The packet relay process uses these fields as follows:

1. When a router interface receives a BOOTREQUEST packet, the router examines the seconds and hops fields in the packet and compares these values to BootP parameters that you configured on that interface.

   The seconds field contains the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the value of the Timeout Secs. parameter configured on the interface, the router drops the packet.

   The hops field contains the maximum number of hops that a packet can take between the source and destination devices. If the packet has traversed more hops than the value of the hops parameter specified for that interface, the router drops the packet.

2. If the router accepts the packet, it alters the packet by:
   - Incrementing the hops field by 1
   - Writing the IP address of the input interface to the gateway IP address field
3. The router then determines which networks should receive this packet and broadcasts it to other networks through a forwarding route that you specify when you configure the router for BootP services.

   If the BootP packet has to travel to a network through another router, you must specify the forwarding route using one of the following methods:

   - Configure the second router for BootP services.

     In this case, the second router inspects the packet in the same way as the first router, and increments the hops field by 1. The second router will not, however, replace the address in the gateway IP address field, because servers will reply to the first router that received the BOOTREQUEST packet.
   - Configure the first router to forward the BOOTREQUEST packet to a specific server.

     In this case, the router will unicast the BOOTREQUEST packet to the server through normal IP services.
4. Servers on other networks receive the BOOTREQUEST packet and respond with a BOOTREPLY packet. Those servers transmit the BOOTREPLY packets through normal IP services to the address of the first interface that received the BOOTREQUEST packet. That address appears in the gateway IP address field in the BOOTREQUEST packet.
5. When the router that first received the BOOTREQUEST packet receives the BOOTREPLY packet, it examines the gateway IP address field to check that the value in this field is the same as the IP destination address that the server used for the packet. If the addresses differ, the router discards the BOOTREPLY packet.
6. If the router accepts the packet, it examines the flags field and forwards the packet to the client as follows:
   - If the flags field contains the value 1, the client does not know its own IP address. The router broadcasts the BOOTREPLY packets to the IP broadcast address (255.255.255.255).

- If the flags field contains the value 0, the client knows its own IP address, which appears in the client IP address field of the BOOTREPLY packet. The router sends the BOOTREPLY packet to that IP address and the link-layer address that appears in the client hardware address field.

DHCP Overview

DHCP, described in RFC 1541, is an extension of BootP and is built on the client-server mode. DHCP allows designated DHCP servers to automatically assign IP addresses and host names to dynamically configured DHCP clients for a predefined period of time.

The DHCP packet format is based on a BootP packet. As a result, DHCP uses the BootP relay agent to forward DHCP packets. This scheme provides interoperability between the existing BootP clients and DHCP servers. The BootP relay agent uses the same criteria and methods for forwarding both DHCP and BootP packets. For information about the packet relay process, see "BootP Relay Agent Overview" on page 2-10.

Why Use DHCP?

Each DCHP client on the network requires its own IP address and configuration information. The DHCP client's IP address is the identifier that other networked devices use to recognize the client on the network. The client's configuration information includes the network domain name, the address of the network servers and gateways, and the subnet mask.

Without DHCP, each time that you add a client to its network, you must manually assign an IP address and configuration information to the client. When clients change offices or users, or leave the network altogether, the configuration information changes as well.

DHCP facilitates network management by automating and centralizing IP address administration and by providing IP configuration information automatically to each networked device when it is needed.

DHCP can allocate three types of IP addresses to DHCP clients: static DHCP addresses, dynamic DHCP addresses, and static BootP addresses. Table 2-3 describes these types of IP addresses.

Table 2-3. IP Address Types Allocated by DHCP

IP Address Type	Description
Static DHCP address	An address that the DHCP server fixes to a client by a unique key, typically the MAC address.
Dynamic DHCP address	An address that the DHCP server allocates to a client for fixed periods of time, called *lease times*. The client can extend the lease so that it continues to use the same dynamic address. When the client leaves the network, the client typically releases the address, and the DHCP server can assign it to another client.
Static BootP address	An address that a DHCP server allocates dynamically with no fixed time period. Unlike a dynamic DHCP address, a static BootP address has an infinite lease time. When the client leaves the network, it must send a message to the DHCP server to release the address. The address is then available for the DHCP server to reassign.

Dynamic IP Address Allocation

If you have only a limited number of IP addresses in a TCP/IP network, DHCP enables you to efficiently use and reuse IP addresses by implementing a concept called IP *address leasing.* A DHCP client can lease an IP address from a DHCP server for a fixed, configurable period of time. The lease period can range from 1 minute to 99 years. If you have more clients than IP addresses, using shorter leases can prevent you from running out of addresses. If you have more addresses than clients, you can use permanent addresses or you can assign fixed addresses to specific clients.

When a lease expires, the DHCP client can contact the DHCP server to renew the lease. Typically, the client attempts to renew the lease halfway through the lease period. For example, if the client is granted an address with a lease time of 1 hour, it asks to renew the address approximately 30 minutes after the client has started to use it.

If the client does not receive an answer from the DHCP server (perhaps because the server is down), it can attempt to reacquire configuration parameters and an IP address from another server, or let the lease lapse, returning the IP address to a client pool. The *client pool* is a group of one or more client IDs or MAC addresses maintained by a DHCP server.

DHCP Components

The Nortel Networks implementation of DHCP consists of the following components:

- DHCP clients
- DHCP server
- NetID Server Manager

The sections that follow describe these components.

DHCP Clients

A DHCP client is a host that uses DHCP to obtain configuration information, such as an IP address, from a DHCP server.

DHCP Server

A DHCP server is a host that provides IP addresses and configuration parameters to DHCP clients.

NetID Server Manager

The NetID Server Manager operates as an interface for the DHCP server (see Figure 2-8). The NetID Server Manager manages and maintains IP addresses and configuration information, and allocates IP addresses to the DHCP server. The NetID Server Manager polls the database periodically and sends configuration changes to the appropriate DHCP servers. The DHCP servers send updated information to the NetID Server Manager, and the Server Manager stores this information in its database.

For example, when the DHCP server starts up, it connects to the NetID Server Manager and requests its configuration. When the DHCP server assigns an IP address to a client, it sends the client's host name and IP address to the NetID Server Manager. The NetID Server Manager then sends this information to the database.

The NetID Server Manager reduces the load on the database, because each DHCP server is not polling for configuration changes and does not require an active (resource-consuming) connection to the database. It also reduces the load on the network, because it is the only component that polls the database for configuration changes.

BootP/DHCP Relay Implementation

The BootP/DHCP relay implementation allows you to configure a router to act as a BootP relay agent. The BootP relay agent forwards DHCPREQUEST packets to DHCP servers on other subnets and forwards DHCPREPLY packets back to DHCP clients.

You must enable the BootP relay agent on the interface to the subnet to be served and configure it with the IP address of the DHCP server. For more information about configuring a BootP relay agent, see "Specifying Interfaces to Receive and Forward DHCP Packets" on page 5-2.

Figure 2-5 illustrates a BootP/DHCP relay implementation.

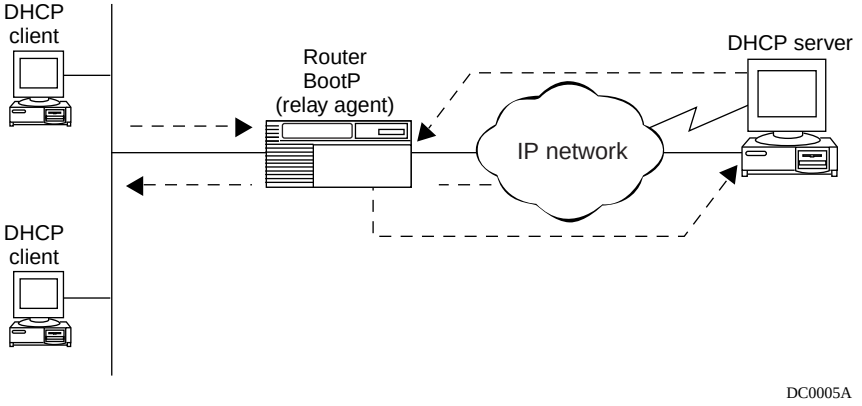

Figure 2-5. BootP/DHCP Relay Implementation

Acquiring an IP Address

A client acquires its IP address from a router configured as a BootP relay agent as follows:

1. Identify DHCP servers.
2. Request and receive IP information.
3. Accept or decline IP information.

The following sections describe each of these stages in detail.

Identifying DHCP Servers

Figure 2-6 shows the first stage of the process of acquiring a new IP address from a router configured as a BootP relay agent.

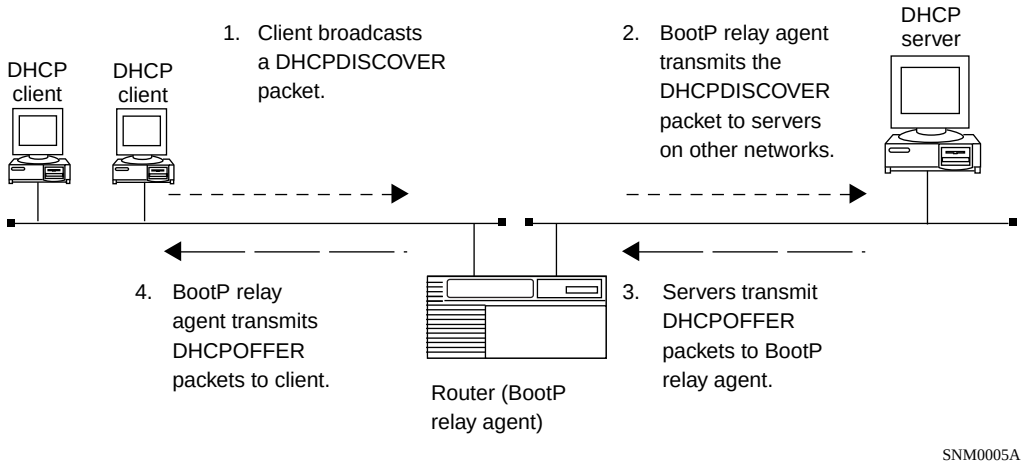
DHCP client
DHCP client
1. Client broadcasts a DHCPDISCOVER packet.
2. BootP relay agent transmits the DHCPDISCOVER packet to servers on other networks.
DHCP server
4. BootP relay agent transmits DHCPOFFER packets to client.
3. Servers transmit DHCPOFFER packets to BootP relay agent.
Router (BootP relay agent)
SNM0005A

Figure 2-6. Identifying DHCP Servers (BootP Relay Agent)

To locate DHCP servers on the network, the DHCP client broadcasts a DHCPDISCOVER packet. Table 2-4 describes the fields in a DHCP packet.

Table 2-4. Fields in a DHCP Packet

Field	Octets	Description
Operation	1	Message operation code or message type. • 1= BOOTREQUEST • 2= BOOTREPLY
Hardware type	1	Hardware address type, for example: 1= 10 Mb Ethernet
Hardware address length	1	Hardware address length, for example: “6” for 10 Mb Ethernet
Hops	1	DHCP client sets to 0.
Transaction ID	4	A random number chosen by the client. The DHCP client and the DHCP server use this number to associate messages and responses exchanged between them.
Seconds	2	The number of seconds that elapsed since a client started trying to boot. The client fills in this number.
Flags	2	If the flags field contains the value 1, the client does not know its own IP address. The router broadcasts the DHCPREPLY packets to the IP broadcast address (255.255.255.255). If the flags field contains the value 0, the client knows its own IP address, which appears in the client IP address field of the DHCPREPLY packet. The router sends the DHCPREPLY packet to that IP address and to the link-layer address that appears in the client hardware address field.
Client IP address	4	The DHCP client IP address. This field is filled in only if the DHCP client is in BOUND, RENEW, or REBINDING state and can respond to ARP requests.
Your IP address	4	DHCP client IP address
Gateway IP address	16	IP address of the DHCP server to use in the next step of the client's bootstrap process. The DHCP server returns this address when it sends DHCPOFFER and DHCPACK messages to the client.

(continued)

Table 2-4. Fields in a DHCP Packet *(continued)*

Field	Octets	Description
Client hardware address	16	The hardware address of the client
Server name	64	Optional DHCP server host name, represented as a null terminated string
File name	128	A boot file name. Represented as a null terminated string in a DHCPDISCOVER message, and a fully qualified directory path name in a DHCPOFFER message.
Options	312	Variable length optional parameters field

The packet relay process uses these fields as follows:

1. The BootP relay agent receives the packet and, if it accepts the packet, transmits it to DHCP servers on other networks.
2. DHCP servers on the local segment see the broadcast packet and respond with a DHCPOFFER packet that includes an available IP address and other configuration information. Before offering the IP address, the DHCP servers may generate an ARP or ICMP echo request on the network to determine whether the IP address is already in use by another device.
3. When a DHCP server offers an IP address, that address is temporarily unavailable to other clients. If the client does not accept or reject the address within a certain period of time, the server reclaims it. The address is then available for other clients.
4. The BootP relay agent receives the DHCPOFFER packet and examines the packet. If the BootP relay agent accepts the packet, it forwards it to the client.
5. If a client does not receive a DHCPOFFER packet within a specified amount of time after broadcasting a DHCPDISCOVER packet, it sends the packet again. The client may rebroadcast the packet a number of times. However, clients operating on systems running Windows® 95 broadcast four DHCPDISCOVER packets, each 2 seconds apart.
6. The client may receive DHCPOFFER packets from several potential servers. If you configure the client to wait for multiple responses, it compares configuration parameters in the DHCPOFFER packets to decide which server to target.

Requesting and Receiving IP Information

Figure 2-7 shows the next stage of the process for acquiring a new IP address from a router configured as a BootP relay agent:

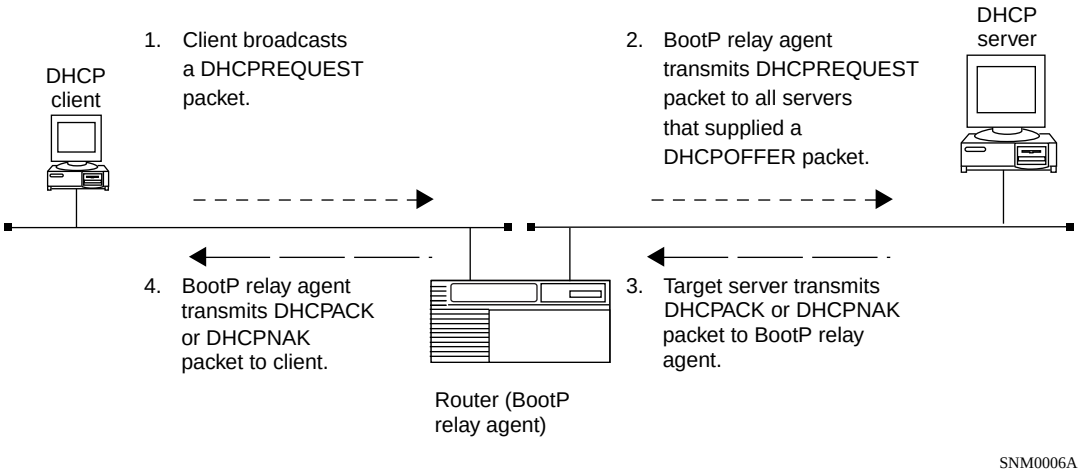
DHCP client
1. Client broadcasts a DHCPREQUEST packet.
2. BootP relay agent transmits DHCPREQUEST packet to all servers that supplied a DHCPOFFER packet.
DHCP server
4. BootP relay agent transmits DHCPACK or DHCPNAK packet to client.
3. Target server transmits DHCPACK or DHCPNAK packet to BootP relay agent.
Router (BootP relay agent)
SNM0006A

Figure 2-7. Requesting and Receiving IP Information (BootP Relay Agent)

1. When the client has chosen a target server, it broadcasts a DHCPREQUEST packet. The DHCPREQUEST packet contains the address of the target server in the server IP address field and the lease offer that it prefers.
2. The router configured as a BootP relay agent receives the packet and forwards it to all servers.
3. Those servers examine the packet, and if their IP addresses differ from the value in the server IP address field, they reclaim the IP addresses that they supplied in the DHCPOFFER packets. These addresses are now available for other clients.

Accepting or Declining IP Information

In a network configuration in which a router is configured as a BootP/DHCP relay agent, the target server recognizes its IP address in the server IP address field, and responds to the DHCPREQUEST packet as follows:

- If the target server can supply the requested configuration parameters, it sends a DHCPACK packet to the client through the BootP relay agent. The DHCPACK packet contains the committed IP address.

The client examines the configuration parameters in the DHCPACK packet and records the duration of the lease period. If the client detects a problem with the configuration parameters, it sends a DHCPDECLINE packet to the server and issues a new DHCPDISCOVER packet. Otherwise, the client accepts the configuration parameters.

- If the target server cannot supply the requested configuration parameters, it sends a DHCPNAK packet to the client through the BootP relay agent.

  When the client receives the DHCPNAK packet, it broadcasts a new DHCPDISCOVER packet and the process begins again.

A client may choose to relinquish its IP address before the lease period expires by sending a DHCPRELEASE packet to the server. This packet contains the relinquished IP address in the client IP address field and the client's MAC address in the client hardware address field.

Reacquiring the Same IP Address

A client may want to reuse an IP address that a server allocated earlier using a BootP relay agent. In this case, the interchange between client and server omits some of the steps described in the previous sections.

The client can acquire the same IP address again using a BootP relay agent by following these steps:

1. The client starts the interchange by broadcasting a DHCPREQUEST packet that contains its previous IP address in the client IP address field.
2. The BootP relay agent receives the packet and forwards it to DHCP servers on other networks.
3. DHCP servers examine the client's configuration parameters in the options field of the DHCPREQUEST packet.
4. The server that originally supplied the configuration parameters recognizes them and responds with a DHCPACK packet.
5. When a client receives a DHCPACK packet, it accepts or declines the parameters, as it would when receiving a new IP address.

If a client's request is invalid (for example, if the client has moved to a new network), servers respond with a DHCPNAK packet. If a client receives only DHCPNAK packets, it must request a new IP address by broadcasting a DHCPDISCOVER packet.

DHCP Server Implementation

The DHCP server implementation allows you to configure a router to act as a DHCP server. In this scenario, the DHCP server, acting in proxy fashion, uses the NetID Server Manager to manage and maintain IP addresses and configuration information stored in its database (Figure 2-8).

The DHCP server uses the information in the database to assign IP addresses and host configuration information to DHCP clients. For more information about configuring a DHCP server, see “Modifying the DHCP Server Configuration” on page 6-2.

Figure 2-8 illustrates a DHCP server implementation.

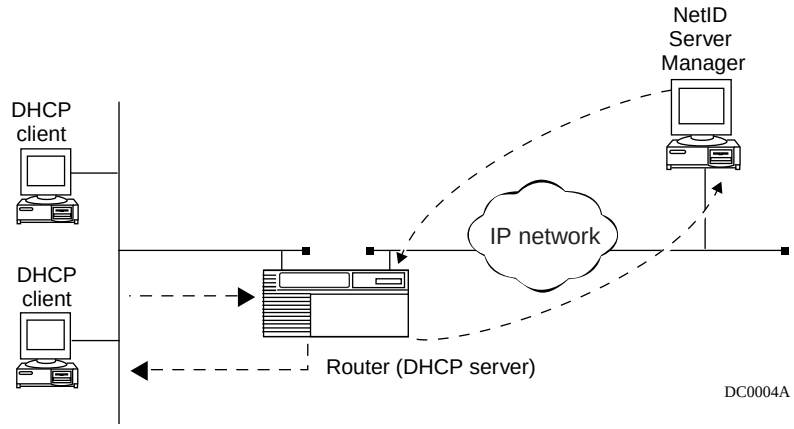

Figure 2-8. DHCP Server Implementation

Acquiring an IP Address

A client acquires its IP address from a router configured as a DHCP server as follows:

1. Identify DHCP servers.
2. Request and receive IP information.
3. Accept or decline IP information.

The following sections describe each of these stages in detail.

Identifying DHCP Servers

Figure 2-9 shows the first stage of the process of acquiring a new IP address from a DHCP server.

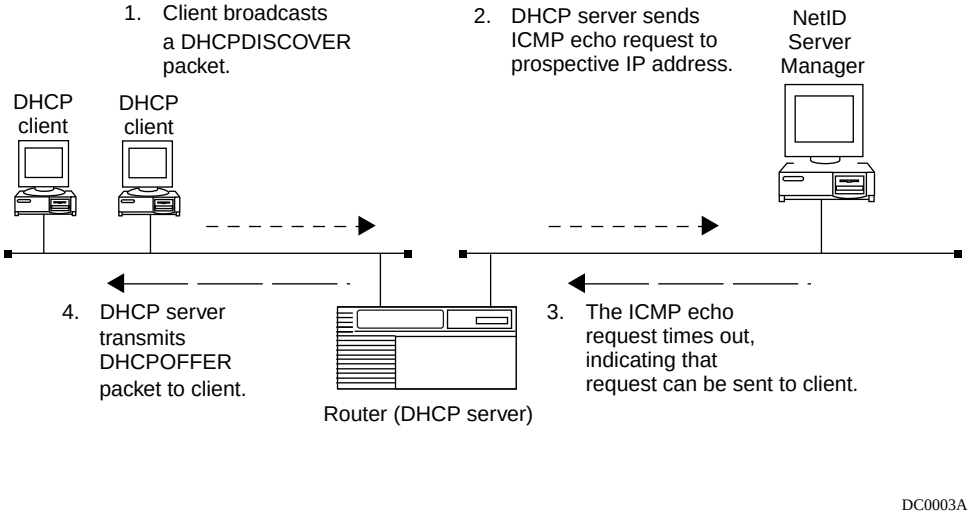
1. Client broadcasts a DHCPDISCOVER packet.
2. DHCP server sends ICMP echo request to prospective IP address.
NetID Server Manager
DHCP client
DHCP client
4. DHCP server transmits DHCPOFFER packet to client.
3. The ICMP echo request times out, indicating that request can be sent to client.
Router (DHCP server)
DC0003A

Figure 2-9. Identifying Routers Configured As DHCP Servers

To identify routers configured as DHCP servers, the DHCP client broadcasts a DHCPDISCOVER packet on its local physical subnet. Table 2-4 on page 2-19 describes the fields in the DHCP packet. The packet release process uses these fields as follows:

1. The router configured as a DHCP server receives the packet and finds an available IP address to assign to the client.
2. The DHCP server sends an ICMP echo request to the prospective IP address to determine whether the address is available. If the DHCP server receives a response, the address is unavailable because it is being used by another host on the network. The DHCP server selects another IP address to offer and sends another ICMP echo request.
3. If there is no response to the ICMP echo request, the DHCP server sends a DHCPOFFER packet that includes an available IP address to the target DHCP client.
4. If a client does not receive a DHCPOFFER packet within a specified amount of time after broadcasting a DHCPDISCOVER packet, it sends the packet again. The client may rebroadcast the packet a number of times. However, clients operating on systems running Windows 95 broadcast four DHCPDISCOVER packets, each 2 seconds apart.
5. The client may receive DHCPOFFER packets from several potential servers. If you configure the client to wait for multiple responses, it compares configuration parameters in the DHCPOFFER packets to decide which server to target.

Requesting and Receiving IP Information

Figure 2-10 shows the next stage of the process of acquiring a new IP address from a DHCP server.

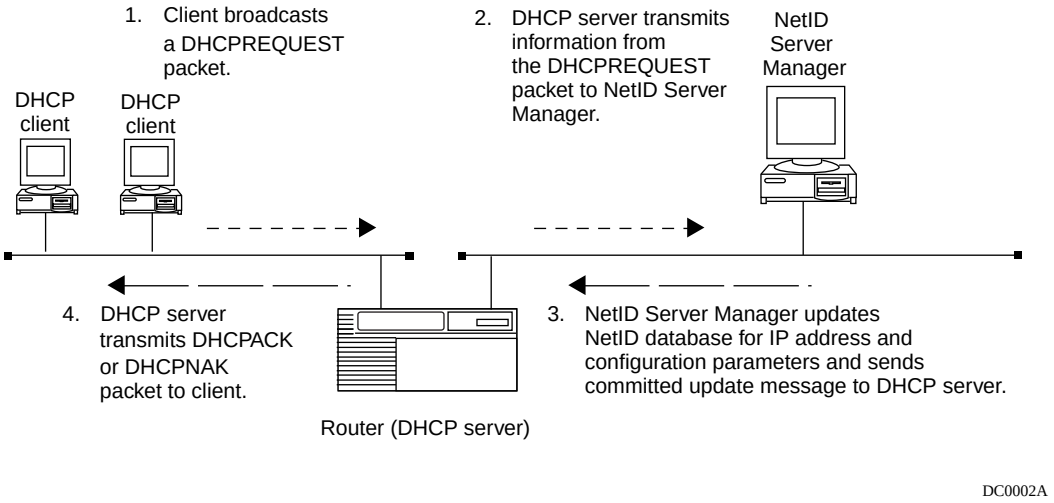
1. Client broadcasts a DHCPREQUEST packet.
2. DHCP server transmits information from the DHCPREQUEST packet to NetID Server Manager.
NetID Server Manager
DHCP client
DHCP client
4. DHCP server transmits DHCPACK or DHCPNAK packet to client.
3. NetID Server Manager updates NetID database for IP address and configuration parameters and sends committed update message to DHCP server.
Router (DHCP server)
DC0002A

Figure 2-10. Requesting and Receiving IP Information (DHCP Server)

1. When the client has chosen a target DHCP server, it broadcasts a DHCPREQUEST packet to the server. The DHCPREQUEST packet contains the address of the target server in the server IP address field.
2. The router configured as a DHCP server examines the packet, and if its IP address differs from the value in the server IP address field, it reclaims the IP address it supplied in the DHCPOFFER packet. This address is now available for other clients.
3. If the DHCPREQUEST packet is valid, the DHCP server forwards the request information to the NetID Server Manager.
4. After the NetID Server Manager updates the NetID database with the new request information, the NetID Server Manager sends a committed update message back to the DHCP server.

Accepting or Declining IP Information

In a network configuration in which the router is configured as a DHCP server, the target server recognizes its IP address in the server IP address field, and responds to the DHCPREQUEST packet as follows:

- If the DHCP server can supply the requested configuration parameters, it sends a DHCPACK packet to the client through the DHCP server.

  The client examines the configuration parameters in the DHCPACK packet and records the duration of the lease period. If the client detects a problem with the configuration parameters, it sends a DHCPDECLINE packet to the server and issues a new DHCPDISCOVER packet. Otherwise, the client accepts the configuration parameters.

- If the target server cannot supply the requested configuration parameters, it sends a DHCPNAK packet to the client through the DHCP server.

  When the client receives the DHCPNAK packet, it broadcasts a new DHCPDISCOVER packet and the process begins again.

Reacquiring the Same IP Address

A client may want to reuse an IP address that a server allocated earlier using DHCP. In this case, the interchange between client and server omits some of the steps described in the previous sections.

The client can acquire the same IP address again using a DHCP server by following these steps:

1. The client starts the interchange by broadcasting a DHCPREQUEST packet that contains its previous IP address in the client IP address field.
2. The DHCP server receives the packet, examines the client's configuration parameters in the options field of the DHCPREQUEST packet, and forwards the client request information to the NetID Server Manager.
3. The NetID Server Manager updates its database and sends a committed update message back to the DHCP server.
4. The DHCP server that originally supplied the configuration parameters recognizes them and responds with a DHCPACK packet.
5. When a client receives a DHCPACK packet from the DHCP server, it accepts or declines the parameters, as it would when receiving a new IP address.

If a client's request is invalid (for example, if the client has moved to a new network), servers respond with a DHCPNAK packet. If a client receives only DHCPNAK packets, it must request a new IP address by broadcasting a DHCPDISCOVER packet.

Chapter 3
Customizing SNMP

This chapter describes how to customize SNMP services. It assumes that you configured an IP interface using the default parameters, as described in Chapter 1, “Starting SNMP, BootP, and DHCP Services,” and that you understand the SNMP concepts in Chapter 2, “SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts.”

Topic	Page
Configuring SNMP Using the BCC and Site Manager	3-2
Customizing SNMP Global Parameters	3-3
Adding SNMP Communities	3-9
Configuring SNMP Community Managers	3-13
Configuring SNMP View-Based Access Control	3-19
Configuring Traps on the Router	3-25
Configuring Thresholds	3-31

Configuring SNMP Using the BCC and Site Manager

Table 3-1 lists the SNMP configuration tasks described in this chapter and indicates whether you can use the BCC or Site Manager to perform each task.

Table 3-1. SNMP Configuration Tasks

Task	BCC	Site Manager
Disabling and Reenabling SNMP	✓	✓
Enabling and Disabling the SNMP Lock Mechanism	✓	✓
Specifying a Lock Address	✓	
Specifying a Lock Timeout Value	✓	✓
Enabling and Disabling Authentication Failure Traps	✓	✓
Specifying the Type of Service for SNMP Packets	✓	
Specifying an SNMP Community Name	✓	✓
Specifying Community Access Privileges	✓	✓
Deleting an SNMP Community	✓	✓
Adding a Manager	✓	✓
Configuring a Manager to Receive Traps	✓	✓
Deleting a Manager	✓	✓
Configuring, Listing, and Deleting a View	✓	
Configuring Communities and Their View Associations	✓	
Configuring Traps on the Router	✓	✓
Disabling a Trap Entity	✓	✓
Configuring Trap Exceptions	✓	✓
Deleting Trap Exceptions	✓	✓
Disabling and Reenabling Thresholds		✓
Setting the Threshold Polling Interval		✓
Adding a Threshold		✓
Enabling and Disabling Thresholds for a Variable		✓
Specifying a Value for the Threshold Level		✓
Specifying the Severity Level for Event Messages		✓
Specifying Threshold Units		✓

(continued)

Table 3-1. SNMP Configuration Tasks *(continued)*

Task	BCC	Site Manager
Determining When to Record Threshold Events		✓
Specifying the Maximum Number of Successive Alarms		✓
Specifying Polling Intervals for Held Variables		✓
Specifying a Threshold Object Name		✓

Customizing SNMP Global Parameters

You can enable SNMP services most easily by accepting all the default parameter values. However, you may want to change these values, depending on your network requirements.

Disabling and Reenabling SNMP

When you enable IP on an interface, SNMP access is automatically enabled through that interface. You can disable and reenable SNMP on the router.

Using the BCC

To disable SNMP, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

disable

For example, the following command disables SNMP:

```
snmp# disable
```

To reenable SNMP, navigate to the SNMP prompt and enter:

enable

For example, the following commands reenable SNMP and display its default values:

```
snmp# enable
snmp# info
    lock enabled
    lock-address 0.0.0.0
    lock-timeout 2
```

```
   authentication-traps enabled
   type-of-service reliability
   state enabled
snmp#
```

Using Site Manager

To disable or reenable SNMP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Global**.	The Edit SNMP Global Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **OK**.	You return to the Configuration Manager window.

Caution: When you disable the SNMP agent in dynamic mode, you immediately prohibit Site Manager from communicating with the router and disconnect your Site Manager session.

Enabling and Disabling the SNMP Lock Mechanism

The SNMP lock mechanism prohibits the SNMP agent from responding to multiple network management stations issuing simultaneous SNMP **set** commands to the router. The SNMP lock mechanism is enabled by default.

If this lock is enabled, the SNMP agent identifies the station from which it receives the next SNMP **set** command and, for a specified time, responds only to SNMP **set** commands from that station. If the agent receives an SNMP **set** command from another network management station during this time, it issues an SNMP genErr GetResponse PDU, which that station logs as an SNMP Set Error message.

To allow the SNMP agent to respond to simultaneous SNMP **set** commands from multiple network management stations, disable the SNMP lock mechanism.

Using the BCC

To disable the lock mechanism, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

lock disabled

To reenable the lock, navigate to the SNMP prompt and enter:

lock enabled

Using Site Manager

To enable or disable the SNMP lock mechanism, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Global**.	The Edit SNMP Global Parameters window opens.
5. Set the **Use Lock** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying a Lock Address

The default lock address is 0.0.0.0. Using the BCC, you can specify a different lock address by navigating to the SNMP prompt (for example, **box; snmp**) and entering:

lock-address <*address*>

address is an IP address in dotted-decimal notation.

For example, the following command sets the lock address to 192.32.15.55:

```
snmp# lock-address 192.32.15.55
snmp#
```

Specifying a Lock Timeout Value

If the SNMP lock mechanism is enabled, you can customize the lock timeout period. The lock timeout period is the maximum number of minutes that the SNMP agent allows an idle network management station to hold a lock on it. During this time, the SNMP agent locks out SNMP **set** commands from other network management stations. The lock timer is reset each time the locking manager issues an SNMP **set** command.

By default, the SNMP agent allows an idle network management station to hold a lock on it for 2 minutes. To change the default lock timeout period, specify a value from 1 through 60 minutes.

Using the BCC

To reset the lock timeout value, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

lock-timeout <*integer*>

integer is the number of minutes.

For example, the following command sets the lock timeout period to 3 minutes:

```
snmp# lock-timeout 3
snmp#
```

Using Site Manager

To reset the lock timeout value, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Global**.	The Edit SNMP Global Parameters window opens.
5. Set the **Lock TimeOut** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling Authentication Failure Traps

The router generates an authentication failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.

When you enable the authentication failure traps feature on the router, you must configure an SNMP community manager to receive the trap (see "Configuring SNMP Community Managers" on page 3-13).

You can prohibit the router from generating authentication failure traps by disabling the authentication failure trap feature.

Using the BCC

By default, SNMP sends an authentication failure trap for sets from a false manager or community. To disable authentication traps, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

authentication-traps disabled

For example, the following command prohibits SNMP from sending authentication failure traps from a false manager or community:

```
snmp# authentication-traps disabled
snmp#
```

To reenable authentication failure traps, navigate to the SNMP prompt and enter:

authentication-traps enabled

For example, the following command causes SNMP to generate authentication failure traps from a false manager or community:

```
snmp# authentication-traps enabled
snmp#
```

Using Site Manager

To enable or disable authentication failure traps, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Global**.	The Edit SNMP Global Parameters window opens.
5. Set the **Authentication Failure Traps** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Type of Service for SNMP Packets

Using the BCC, you can specify the type of service in which SNMP packets will be generated by setting the type of service to either reliability or normal. For SNMP, high-reliability type of service is important.

By default, the type of service is set to reliability. To specify the type of service, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

type-of-service {**reliability** | **normal**}

For example, the following command causes SNMP to generate packets with a type of service of reliability:

```
snmp# type-of-service reliability
snmp#
```

Adding SNMP Communities

An *SNMP community* is a logical relationship between an SNMP agent and one or more SNMP managers. The community has a name, and all members of a community have the same access privileges: either *read-only* (members can view configuration and performance information) or *read-write* (members can view configuration performance information, and also change the configuration).

This section describes how to add and delete the SNMP communities to which the SNMP agent responds or sends traps.

Specifying an SNMP Community Name

You can add SNMP communities by specifying the name of the community. The community name can consist of up to 63 characters, including embedded spaces.

Using the BCC

To create a community name, navigate to the SNMP prompt (for example, **box; snmp**) and enter:

community *<name>*

name is any string of printable ASCII characters, up to 63 characters in length, including embedded spaces.

For example, the following commands create a community named “router1” and display its default values:

```
snmp# community router1
community/router1# info
    label router1
    access read-only
    scope-type {}
```

Using Site Manager

To specify the name of a community, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Choose **Community**.	The Community menu opens.
6. Choose **Add Community**.	The Add SNMP Community window opens.
7. Set the **Community Name** parameter. Click on **Help** or see the parameter description on page A-5.	
8. Click on **OK**.	You return to the SNMP Community List window.

Specifying Community Access Privileges

After you specify the name of the community, you must assign access privileges to all members of the community. You can specify one of two types of access privileges to each community that you define: read-only or read-write.

By default, the router grants read-only access privileges to all members of an SNMP community. Read-only access allows members of a community to view configuration and performance information. Set this parameter to read-write to allow members of a community to view configuration and performance information, and also to change the configuration of a router.

Using the BCC

By default, the community has read-only access. To specify the type of access, navigate to the community-specific prompt (for example, **box; snmp; community/router1**) and enter:

access {**read-write** | **read-only**}

For example, the following command allows read-write access to the community "router1":

```
community/router1# access read-write
community/router1#
```

Using Site Manager

To specify the access privilege for a community, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Choose **Community**.	The Community menu opens.
6. Choose **Edit Community**.	The Edit SNMP Community window opens.
7. Set the **Access** parameter. Click on **Help** or see the parameter description on page A-5.	
8. Click on **OK**.	You return to the SNMP Community List window.

Deleting an SNMP Community

You can delete an SNMP community to which the agent responds or sends traps.

Using the BCC

To delete an SNMP community, navigate to the community-specific prompt (for example, **box; snmp; community/router1**) and enter:

delete

For example, the following command deletes the community "router1":

```
community/router1# delete
snmp#
```

Using Site Manager

To delete an SNMP community, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Select the community that you want to delete.	
6. Choose **Community**.	The Community menu opens.
7. Choose **Delete Community**.	The Delete SNMP Community window opens.
8. Verify that the correct community name appears in the window. Click on **Cancel** if you do not want to delete the selected community.	
9. Click on **Delete**.	The Configuration Manager removes the community from the list.

Configuring SNMP Community Managers

This section describes how to add and delete SNMP community members (managers). It also describes how to configure managers to receive traps from the SNMP agent.

Adding a Manager

After you add a community name on the router and assign access privileges to it, you can add one or more community members (called *managers*). By default, the IP address 0.0.0.0 is a manager in the public community.

Note: When you add the first IP interface, Site Manager automatically creates a read-write public community with a wildcard manager (0.0.0.0). For security reasons, you should replace the public community and wildcard manager with a unique community specifying a limited list of managers.

Using the BCC

To add a manager to a community, navigate to the community prompt (for example, **box; snmp; community/router1**) and enter:

manager address *<ip_address>*

For example, the following command creates a manager with an IP address of 2.2.2.2 and assigns it to the community router1:

```
community/router1# manager address 2.2.2.2
manager/router1/2.2.2.2#
```

Using Site Manager

To add a manager to a particular community, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Choose **Community**.	The Community menu opens.
6. Choose **Managers**.	The SNMP Manager List window for that community opens.
7. Choose **Manager**.	The Manager menu opens.
8. Choose **Add Manager**.	The Add SNMP Manager window opens.
9. Enter the IP address of the SNMP manager that you want to add.	
10. Click on **OK**.	The Configuration Manager adds the manager to the community.

Configuring a Manager to Receive Traps

After you add a manager to a community, you can configure the manager to receive traps by specifying its UDP port number and the types of traps that the agent sends to that manager.

When you configure a manager to receive specific traps or all traps (see Table 3-2 on page 3-16), the router sends this manager all enabled event traps. There is no MIB correspondence between a specific SNMP manager and a trap entity. Rather, all SNMP managers that you configure to receive specific traps receive all traps that you configure.

Specifying the Trap Port

By default, the standard port number on the managing station to which the SNMP agent transmits traps is 162. To use a different UDP port number, specify a value from 1 through 9999. Do not specify a port that another application uses.

Using the BCC

To specify the UDP port number on the managing station to which the SNMP agent sends traps, navigate to the manager-specific prompt (for example, **box; snmp; community/router1; manager/router1/2.2.2.2**) and enter:

trap-port *<integer>*

integer is a number from 1 through 9999.

For example, the following command causes the SNMP agent to send traps to manager 2.2.2.2 on port number 150:

```
manager/router1/2.2.2.2# trap-port 150
manager/router1/2.2.2.2#
```

Using Site Manager

To specify the UDP port number on the managing station to which the SNMP agent sends traps, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Choose **Community**.	The Community menu opens.
6. Choose **Managers**.	The SNMP Manager List window for that community opens.
7. Select the manager that you want to edit.	
8. Choose **Manager**.	The Manager menu opens.
9. Choose **Edit Manager**.	The SNMP Manager window opens.
10. Set the **Trap Port** parameter. Click on **Help** or see the parameter description on page A-6.	
11. Click on **OK**.	You return to the SNMP Manager List window.

Specifying a Trap Type

You can specify one of four types of traps that the SNMP agent can send to the manager: generic, specific, all, or none. Table 3-2 describes these trap options.

Table 3-2. Trap Types Sent by the SNMP Agent

Trap Type	Description
Generic	This is the default trap type. It sends the well-defined SNMP traps (cold-start, warm-start, and authentication failure traps) to the manager. The cold-start and warm-start traps are automatically active in the SNMP agent; however, you must enable the Authentication Failure Traps global parameter for the agent to send such traps to a specified manager.
Specific	Allows you to configure the agent software to send all enabled log event traps to a specified manager
All	Allows you to send cold-start and warm-start traps, and all enabled log event traps, to a specified manager
None	Prohibits the SNMP agent from sending traps to a specified manager

Using the BCC

By default, the SNMP agent sends generic traps to the manager. To specify a different type of trap, navigate to the manager-specific prompt (for example, **box; snmp; community/router1; manager/router1/2.2.2.2**) and enter:

traps *<trap_type>*

trap_type is one of the following:

generic
specific
all
none

For example, the following command causes the SNMP agent to send specific traps to manager 2.2.2.2:

```
manager/router1/2.2.2.2# traps specific
manager/router1/2.2.2.2#
```

Using Site Manager

To specify a trap type, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Choose **Community**.	The Community menu opens.
6. Choose **Managers**.	The SNMP Manager List window for that community opens.
7. Select the manager that you want to edit.	
8. Choose **Manager**.	The Manager menu opens.
9. Choose **Edit Manager**.	The SNMP Manager window opens.
10. Set the **Trap Types** parameter. Click on **Help** or see the parameter description on page A-6.	
11. Click on **OK**.	You return to the SNMP Manager List window.

Deleting a Manager

You can delete a manager from its associated community by deleting the manager's IP address from the list of SNMP managers.

Using the BCC

To delete a manager, navigate to the manager-specific prompt (for example, **box; snmp; community/router1; manager/router1/2.2.2.2**) and enter:

delete

For example, the following command deletes the manager 2.2.2.2 from the community router1:

```
manager/router1/2.2.2.2# delete
community/router1#
```

Using Site Manager

To delete a manager, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Communities**.	The SNMP Community List window opens.
5. Select the community from which you want to delete the manager.	
6. Choose **Community**.	The Community menu opens.
7. Choose **Managers**.	The SNMP Manager List window for that community opens.
8. Select the manager that you want to delete.	
9. Choose **Manager**.	The Manager menu opens.
10. Choose **Delete Manager**.	The Delete SNMP Manager window opens.
11. Make sure that the correct manager IP address appears.	
12. Click on **Delete**.	The Configuration Manager removes the manager from the community.

Configuring SNMP View-Based Access Control

The SNMP view-based access control feature allows you to modify what can or cannot be seen of a router's MIB tree. You can include or exclude from a view any MIB object, attribute, or instance in the router's MIB. You can also include or exclude access to a MIB subtree for traps, and to the SNMP operations **get**, **get-next**, and **set**.

Note: Because of the way that SNMP works, the SNMP **get-next** function does not allow you to exclude an attribute and include subsequent attributes. When you exclude an attribute, all subsequent attributes are also excluded. For example, if you have six attributes, and you exclude the second attribute, you are really excluding attributes 2 through 6; you will not be able to view attributes 2 through 6.

When you configure a view, you specify *view subtrees* -- that is, instructions for what MIB information the agent will allow to be seen and not seen by managers in the specified community.

This feature also lets you manage overlapping private address spaces. For example, if two routers use the same IP address, you can create a view that excludes the MIB of one address. Then, when the management station queries the MIB for information, it receives information only from the router whose view you did not exclude.

You can configure SNMP view-based access control using the BCC or the Technican Interface.

Configuring, Listing, and Deleting a View

To configure, list, or delete a view and its contents, use the **snmpserver view** command. You can enter this command at the BCC or Technician Interface prompt.

Configuring a View

When you configure a view, you control access to a MIB subtree. To configure a view, enter the following command:

snmpserver view {*<view_name>*} {*<oid_tree>*} {**included** | **excluded**}

- *view_name* is the name that you assign to this particular view.
- *oid_tree* specifies the portions of the MIB that you want to include or exclude.
- **included** specifies that *oid_tree* is to be included in this view.
- **excluded** specifies that *oid_tree* is to be excluded from this view.

If you specify the *oid_tree* argument in the **snmpserver view** command**,** you can use wildcards. You can use one wildcard with any portion of the *oid_tree*, and a second wildcard at the end of the *oid_tree*. The first wildcard affects the attribute portion of the subtree, and the second wildcard affects the instance portion of the subtree. A match on an incoming SNMP OID is made on the longest matching MIB subtree.

The following examples illustrate the use of wildcards.

Entering this Value for <oid_tree>	Includes or Excludes in the View
wfIpIntfCfgEntry.*.192.32.140.1.1	All attributes of wfIpIntfCfgEntry
wfIpIntfCfgEntry.* or **wfIpIntfCfgEntry**	All instances of wfIpIntfCfgEntry
wfIpIntfCfgEntry.1.*	All instances of wfIpIntfCfgEntry with an attribute ID of 1
wfIpIntfCfgEntry.1.192.32.*	All instances of wfIpIntfCfgEntry with an attribute of 1 that have an instance ID that begins with 192.32.
wfIpIntfCfgEntry.*.192.32.*	All attributes of wfIpIntfCfgEntry that have an instance ID that begins with 192.32.

For example, the following command creates a view named “block,” which will exclude any attributes of wfIpIntfCfgEntry for the IP address 192.32.140.1.1:

snmpserver view block wfIpIntfCfgEntry.*.192.32.140.1.1 excluded

When multiple view subtrees are configured within a view, an incoming SNMP OID will match on the longest matching subtree in the view. For example, in looking for a match against the *oid_tree* value wfIpIntfCfgEntry.1.192.32.140.1.1, SNMP will bypass the subtree that is excluded, and then match on all values in the included *oid_tree* for subtree 2.

oid_tree value for subtree 1: **wfIPIntfCfgEntry excluded**

oid_tree value for subtree 2: **wfIPIntfCfgEntry.*.192.32.140.1.1 included**

Listing All Views or the Contents of a View

To list all configured views or the contents (MIB subtrees) of a particular view, enter:

snmpserver view [*<view_name>*] **list**

- *view_name* is the name of the view for which you want to display MIB subtrees. If you do not specify the argument *view_name*, the command displays the names of all configured views.
- **list** displays all MIB subtrees that belong to a view, or the names of all configured views, depending on whether you specify *view_name.*

For example, to display all subtrees that belong to a view named “block,” enter:

snmpserver view block list

This command displays the following subtree information for that view:

```
View Subtree                        View Type     Subtree Index
wfIpIntfCfgEntry.*.192.32.140.1.1 Excluded      1.1
```

To display the names of all configured views, enter:

snmpserver view list

The command displays the following:

```
View Index                    View Name
1                             block
```

Deleting a View or Its Contents

To delete a view or the contents (MIB subtrees) belonging to a particular view, enter:

snmpserver view {<*view_name*>} [<*oid_tree*>] **delete**

- *view_name* is the name of the view that you want to delete, or from which you want to delete MIB subtrees.
- *oid_tree* specifies the MIB subtree that you want to delete from *view_name*. If you do not specify *oid_tree*, then this command will delete the view itself, including all subtree associations.
- **delete** deletes a view, or deletes a MIB subtree from a view, depending on whether you specify *oid_tree*.

For example, to delete the entire view named “block,” enter:

snmpserver view block delete

By specifying *oid_tree* to delete a particular MIB subtree from a view, you also delete the “include” or “exclude” action associated with the subtree that you specified when you configured the view.

For example, to delete the *oid_tree* identified by wfIpIntfCfgEntry.*.192.32.140.1.1 and its associated include or exclude action from the view named “block,” enter:

snmpserver view block wfIpIntfCfgEntry.*.192.32.140.1.1 delete

Configuring Communities and Their View Associations

To configure a community, associate and disassociate a view with the community, list community information, or to delete a community, you use the **snmpserver community** command. You can enter this command at the BCC or Technician Interface prompt. The **snmpserver community** commands also work with any communities that you may have already created.

An *SNMP community* is a logical relationship between an SNMP agent and one or more SNMP community managers. The agent establishes one community for each combination of authentication and access control characteristics that you choose.

Configuring a Community

To configure a community, enter the following command:

snmpserver community {<*community_name*>} {**RO** | **RW**}

- *community_name* is the name that you give to this community.
- **RO** specifies read-only access to the viewable MIBs for this community.
- **RW** specifies read-write access to the viewable MIBs for this community.

For example, to create a community named “pubnet” that is configured to allow read-write access, enter:

snmpserver community pubnet RW

Associating a View with a Community

Although a view can be associated with multiple communities, each community can be associated with only one view. To associate a view with a community, enter the following command:

snmpserver community {<*community_name*>} **view** {<*view_name*>}

- *community_name* is the name of the community with which you want to associate the view.
- *view_name* is the name of the view that you are associating with the community.

For example, to associate the view named “block” with the community name “pubnet” allowing read-write community access, enter:

snmpserver community pubnet view block

Listing Community Information

To list information (index, name, associated view, and access rights) for a specific community, or for all configured communities, enter:

snmpserver community [<*community_name*>] **list**

- *community_name* is the name of the community for which you want to display this information. If you do not specify the *community_name* argument, the command displays information for all configured communities.

- **list** displays information for a particular community or for all communities, depending on whether you specify the *community_name* argument.

For example, to list information for a community named “pubnet,” enter:

snmpserver community pubnet list

The command displays the following:

```
Community      Community     Associated
Index          Name          View            Access

2              pubnet        block           read-write
```

To see a complete list of all configured communities, enter the following command. Note that a community named public is always configured by default.

snmpserver community list

The command displays the following:

```
Community      Community
Index          Name          Associated View   Access

1              public        none              read-write
2              pubnet        block             read-write
3              private       secret            read-only
```

Disassociating a View from a Community

You can disassociate a view from a community or delete a community record, which automatically removes the view association. To disassociate a view from a community, enter:

snmpserver community{*<community_name>*} [**view** *<view_name>*] **delete**

- *community_name* is the name of the community from which you want to disassociate a view.
- *view_name* is the name of the view that you want to disassociate from the community. If you do not specify *view_name*, then the command deletes the specified community entirely.

- **delete** disassociates a view from a community or deletes the community, depending on whether you specify *view_name*.

For example, to disassociate the view named “block” from the community “pubnet,” enter:

snmpserver community pubnet view block delete

To delete the community named “pubnet,” and thereby the view association with “pubnet,” enter:

snmpserver community pubnet delete

Configuring Traps on the Router

A *trap* is an event that the router sends to some external network device, such as a network management station. You can specify which log events the SNMP agent sends to the network management station as traps, based on the following:

- *Slot number*: the number of the slot on which the trap will be received
- *Entity number*: the code assigned to the entity issuing the event that uniquely identifies a router event
- *Severity level*: indicates whether the trap is a fault, warning, information, trace, or debug message

A router never broadcasts traps on the network. Rather, it sends traps to specific IP addresses, which you configure on the router as managers of a community. Traps are always sent to specific managers. For more information about traps, see “Events and Traps” on page 2-5.

Using the BCC

To specify a trap entity based on slot and protocol entity, enter the following command at the SNMP prompt:

trap-entity entity <*entity_name*> **slot** <*slot_number*>

entity_name is the name of the entity issuing the event. For a list of all entities, enter **help trap-entity entity** at the SNMP prompt.

slot_number is the number of the slot on which the trap will be received.

For example, the following command causes the SNMP agent to send to a network management station a trap for the IP protocol on slot 2:

```
snmp# trap-entity entity ip slot 2
trap-entity/ip/2#
```

By default, the attribute for all severity levels is set to **off**. To turn on logging for any severity level, navigate to the trap entity-specific prompt (for example, **box; snmp; trap-entity/ip/2**) and enter one or more of the following commands:

fault-log on
warning-log on
information-log on
trace-log on
debug-log on

For example, to send warning and fault traps to the network management station, enter the following commands:

```
trap-entity/ip/2# warning-log on; fault-log on
```

Using Site Manager

To specify a trap entity, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Trap Configuration**.	The Trap Configuration menu opens.
5. Choose **Interfaces**.	The Trap Configuration window opens.
6. Select the slot for which you want to configure traps by clicking on the bar in the Slot box.	
7. Select an entity for which you want to configure traps. If you want to configure traps for all entities running on the slot, choose **All Entities** from the top of the column.	The entity names appear in the Available Entities column, a comprehensive list of all protocols available, regardless of the platform or software that you are using.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
8. Select the severity level at which you want to receive traps by clicking on the Events box at the bottom of the window. For a description of severity levels, see "Severity Levels" on page 2-6.	
9. Click on **Update**.	The entity name moves to the Current Entities column, indicating that you want to receive traps for this entity at the severity level that you specified. (To move an entity from the column, select the entity name and then click on **Remove**.)
10. Repeat steps 6 through 9 for other slots that you want to configure.	
11. Click on **Save**.	You return to the Configuration Manager window.

Disabling a Trap Entity

You can prevent the SMNP agent from sending a specific trap entity to a network management station regardless of slot by disabling the trap entity.

Using the BCC

Trap entities are enabled by default. To prevent the SMNP agent from sending a specific trap entity to a network management station regardless of slot, navigate to the trap entity-specific prompt (for example, **box; snmp; trap_entity/ip/2**) and enter the following command:

disable

For example, the following command prevents the SNMP manager from sending traps for the IP entity on slot 2:

```
trap-entity/ip/2# disable
trap-entity/ip/2#
```

Using Site Manager

To disable a trap entity, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Trap Configuration**.	The Trap Configuration menu opens.
5. In the Current Entities column, select the entity name that you want to delete.	The entity name that you selected is highlighted.
6. Click on **Remove**.	The entity name is removed from the Current Entities column.
7. Click on **Save**.	Site Manager saves the changes that you made.

Configuring Trap Exceptions

You can configure up to 50 trap exceptions, which specify that the SNMP agent always sends or never sends traps to the network management station, regardless of the trap configuration settings and regardless of the slot that you specified.

You configure a trap exception by specifying the following:

- Entity code for the event for which you want to configure an exception
- Code of the event for which you want to configure an exception
- Whether the SNMP agent always sends or never sends a trap to the network management station (Site Manager only)

To access the event message database, look on the documentation CD that comes with BayRS or look on the Web at *support.baynetworks.com/library/tpubs/events*.

Using the BCC

To specify a trap exception based on protocol entity and event code, enter the following command at the SNMP prompt:

trap-event entity *<entity_name>* **event** *<event_code>*

entity_name is the name of the entity issuing the message. For a list of all entities, enter **help trap-event entity** at the SNMP prompt.

event_code is the numerical value assigned to the event message.

For example, the following command causes the SNMP agent to send to a network management station a trap for the IP protocol generating messages for interfaces that transition to the down state (event code 3):

```
snmp# trap-event entity ip event 3
trap-event/ip/3# info
   entity ip
   event 3
   state enabled
snmp#
```

Using Site Manager

To configure a trap exception, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu open.
3. Choose **SNMP**.	The SNMP menu opens.
4. Choose **Trap Configuration**.	The Trap Configuration menu opens.
5. Choose **Exceptions**.	The Trap Exceptions List window opens.
6. Click on **Add**.	The Add Trap window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Set the following parameters: • **Entity Code** • **Event Code** • **Always/Never Trap** Click on **Help** or see the parameter descriptions beginning on page A-7.	
8. Click on **OK**.	You return to the Trap Exceptions List window.

Deleting Trap Exceptions

You can delete a trap exception by specifying the entity name and the event code for the trap event.

Using the BCC

To delete a trap exception, navigate to the trap-exception prompt (for example, **box; snmp; trap-event/ip/3**) and enter:

delete

For example, the following command deletes the trap exception for IP protocol event code 3:

```
trap-event/ip/3# delete
snmp#
```

Using Site Manager

To delete a trap exception, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **SNMP**.	The SNMP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Trap Configuration**.	The Trap Configuration menu opens.
5. Choose **Exceptions**.	The Trap Exceptions List window opens.
6. Select the trap exception that you want to delete.	
7. Click on **Delete**.	
8. Click on **Done**.	You return to the Configuration Manager window.

Configuring Thresholds

Using Site Manager, you can configure thresholds for any integer, counter, gauge, or time-tick variable in the MIB. For more information about using thresholds, see “Thresholds” on page 2-7.

To configure a threshold, you must have a good understanding of the MIB and be able to identify the instances of MIB objects to which you want to apply a threshold. For complete information about identifying a MIB object or an instance identifier, see the statistics chapter of *Configuring and Managing Routers with Site Manager.*

Disabling and Reenabling Thresholds

By default, the thresholds feature is enabled on all interfaces on which IP is configured.

To disable and reenable thresholds, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Global**.	The Edit Thresholds Global Parameters window opens.
5. Set the **Enable/Disable** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Threshold Polling Interval

The threshold polling interval sets the time interval at which the agent polls the variable to determine whether that variable has reached a threshold. You must set a minimum polling interval of 5 seconds; there is no maximum value. The default polling interval is 60 seconds.

When setting a polling interval, remember that the more often the agent polls the variable, the more memory it needs to manage the thresholds for this statistic.

To set the threshold polling interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Global**.	The Edit Thresholds Global Parameters window opens.
5. Set the **Polling Interval** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **OK**.	You return to the Configuration Manager window.

Adding a Threshold

To add a threshold, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Click on **Add**.	The Threshold Configuration window opens, displaying a list of all MIB objects that the agent supports.
6. Select the object to which you want to apply a threshold.	The object appears in the Object field.
7. Enter the instance identifier in the Instance field.	
8. Click on **Save**.	You return to the Threshold Interface Lists window.
9. Click on **Apply**.	
10. Repeat steps 5 through 9 to add other thresholds.	
11. Click on **Done** when you have finished adding thresholds.	You return to the Configuration Manager window.

Enabling and Disabling Thresholds for a Variable

You can decide whether to turn the threshold for a specific variable on or off by setting the Threshold Enable parameter.

To tell the agent to apply the threshold to a variable, specify Enable. To tell the agent to ignore the threshold for a variable, specify Disable.

To enable or disable thresholds for a variable, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold Enable** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying a Value for the Threshold Level

You can specify an integer value that determines the level (low, medium, or high) at which you want the agent to generate a threshold exception event for a variable.

To specify a value for the threshold level, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the following parameters: • **Threshold Low Value** • **Threshold Medium Value** • **Threshold High Value** Click on **Help** or see the parameter descriptions beginning on page A-10.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Severity Level for Event Messages

You can specify the severity level of the event message that the agent generates when a variable exceeds a low, medium, or high threshold level.

You can specify one of these severity levels:

- *Information:* allows low, medium, or high threshold exceptions to generate routine events that require no action.
- *Warning:* allows low, medium, or high threshold exceptions to generate events that indicate that an unexpected situation occurred.
- *Debug:* allows low, medium, or high threshold exceptions to generate events that you can use to solve network problems.

To specify the severity level for event messages, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the following parameters: • **Threshold Low Event Level** • **Threshold Medium Event Level** • **Threshold High Event Level** Click on **Help** or see the parameter descriptions beginning on page A-10.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying Threshold Units

You can specify the units used to determine whether a variable has exceeded a threshold.

- To generate a threshold event when the variable's rate of change *per second* reaches a threshold, set the Threshold Units parameter to Persecond.
- To generate a threshold event when the value of the variable reaches a threshold, set the Threshold Units parameter to Absolute.

To specify threshold units, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold Units** parameter. Click on **Help** or see the parameter description on page A-13.	
6. Click on **Done**.	You return to the Configuration Manager window.

Determining When to Record Threshold Events

You can determine when the agent generates a threshold event by setting the Threshold Action parameter.

By default, the agent generates a threshold event when the value of the variable you specify is *greater than* the threshold that you specify. If you want the agent to generate threshold events when the value of the variable is *less than* the threshold that you specify, set the Threshold Action parameter to Lessthan.

To determine when to record threshold events, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold Action** parameter. Click on **Help** or see the parameter description on page A-13.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Successive Alarms

Successive alarms represent two or more polling periods when the agent generates an alarm as a result of an exception at the same threshold level. By default, the maximum number of successive alarms is set to 5.

You can specify the maximum number of successive alarms that the agent generates for a variable. When the agent exceeds the maximum number of alarms, it marks the threshold as held. The agent generates no more alarms until the variable either crosses the threshold at a different level or crosses no threshold for the number of polling intervals equal to the value of the Threshold HoldDown Intervals parameter.

To specify the maximum number of successive alarms, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold Max Successive Alarms** parameter. Click on **Help** or see the parameter description on page A-14.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying Polling Intervals for Held Variables

You can specify the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held. The lower the number that you specify, the more likely the agent is to generate repetitive event messages for a variable that is intermittently exceeding thresholds.

To specify the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold HoldDown Intervals** parameter. Click on **Help** or see the parameter description on page A-14.	
6. Click on **Done**.	You return to the Configuration Manager window.

Specifying a Threshold Object Name

By default, the ASN.1 object identifier is the object name that appears in the threshold event message. You can replace the ASN.1 object identifier by specifying a name for the object in string format. The string that you enter appears in the log file, making it easier to identify the object that is the subject of the trap.

To specify a threshold object name, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **Thresholds**.	The Thresholds menu opens.
4. Choose **Thresholds**.	The Thresholds Interface Lists window opens.
5. Set the **Threshold Label** parameter. Click on **Help** or see the parameter description on page A-15.	
6. Click on **Done**.	You return to the Configuration Manager window.

Chapter 4
Customizing BootP

This chapter describes how to customize BootP services. It assumes that you configured an IP interface and started BootP on this interface using the default BootP parameters, as described in Chapter 1, “Starting SNMP, BootP, and DHCP Services” and that you understand the BootP concepts in Chapter 2, “SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts.”

Topic	Page
Customizing BootP Relay Agent Parameters	4-2
Setting Up the Routing Path from the BootP Server to the Router	4-7
Configuring an AN to Use EZ-Install over a Frame Relay PVC	4-13
Specifying Servers for BootP Services	4-14
Deleting the BootP Relay Agent from an IP Interface	4-18
Deleting BootP Globally	4-19

Customizing BootP Relay Agent Parameters

After you configure IP interfaces for BootP services, you can configure BootP relay agent parameters for all of these IP interfaces. The BootP relay agent is responsible for transmitting BOOTREQUEST packets to servers on the network and for transmitting BOOTREPLY packets to clients.

Disabling and Reenabling BootP

When you start BootP on an interface, BootP is automatically enabled on that interface and default values are in effect for all BootP parameters.

To disable or reenable BootP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Set the **Enable/Disable** parameter. Click on **Help** or see the parameter description on page A-16.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Enabling ARP Cache Support

Some boot PROM devices do not support the Address Resolution Protocol (ARP). Without ARP support, the client PC or workstation cannot use the BootP relay agent (that is, the BayRS router configured as a BootP relay agent) to download a file over the network.

To accommodate devices that do not run ARP, you can configure the router to create an ARP cache entry based on the information received in the BootP reply from the server. By default, this feature is disabled.

Note: Enabling or disabling the ARP cache feature has no effect on the operation of DHCP.

Using Site Manager

To enable ARP cache entry support, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Set the **ARP Cache Enable** parameter. Click on **Help** or see the parameter description on page A-18.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Using the Technician Interface

To enable the ARP cache entry feature using the Technician Interface, set the wfBootpRelayIntfArpCache MIB variable to a value of 1. For example, this command sets the BootP relay agent interface ARP cache MIB variable to enabled on interface 10.10.10.1:

s wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.10.10.10.1 1; commit

To disable ARP cache support, set the wfBootpRelayIntfArpCache MIB variable to a value of 2. By default this variable is disabled.

To display the setting of the ARP cache entry MIB variable on all interfaces, enter the following command:

g wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.*

Specifying the Maximum Number of Hops from Client to Server

A *hop* is the logical distance between a source device and a destination device. Source-device combinations can include a BootP relay agent and a BootP server, a client and a BootP relay agent, or two BootP relay agents.

By default, the maximum number of hops that a packet can take from the source device to the destination device (client to server) is four. If the value in the hops field of a BOOTREQUEST packet is greater than the configured maximum value, the router drops the packet.

To specify the maximum number of hops from client to server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Set the **Hops** parameter. Click on **Help** or see the parameter description on page A-16.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Specifying a Minimum Timeout Value

By default, the router immediately forwards BOOTREQUEST packets to the destination address in the BootP relay forwarding table. You can configure the router to wait before forwarding a BOOTREQUEST packet out an interface. If the value in the seconds field of a BOOTREQUEST packet is less than the value configured on the interface, the router drops the packet.

The default minimum timeout value is 0 seconds. You can specify a value from 1 through 65,535 seconds (equivalent to 18 hours, 12 minutes, and 15 seconds).

To specify the minimum timeout value, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Timeout Secs.** parameter. Click on **Help** or see the parameter description on page A-17.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Relay Mode for Packet Forwarding

BootP and DHCP use the BootP relay agent to forward packets. You can configure the BootP relay agent to forward BootP packets, DHCP packets, or both. The default setting is BootP, which allows the interface to transmit only BootP packets. Change the setting if you want to transmit DHCP packets.

To set the relay mode on a BootP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Set the **Pass Through Mode** parameter. Click on **Help** or see the parameter description on page A-17.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting Up the Routing Path from the BootP Server to the Router

You must define the routing path from the BootP server to the router to ensure the transmission of BOOTREQUEST packets from one end of the network to the other. You define this routing path by:

- Enabling BootP forwarding on upstream routers
- Specifying interfaces to receive and relay BOOTREQUEST packets
- Creating a BootP relay agent forwarding table for each router in the path

Enabling BootP on Router Interfaces

Before you enable BootP on router interfaces, make sure that the router is in forwarding mode. Setting the router to forwarding mode allows the BootP relay agent to route (forward) all BOOTREQUEST packets and to process both broadcast packets and all packets explicitly addressed to it. For instructions on configuring the router in forwarding mode, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

You must enable BootP (also called BootP pass-through or gateway) on all interfaces in the paths between the routers and the BootP server. For example, you would enable BootP on the interfaces indicated in Figure 4-1.

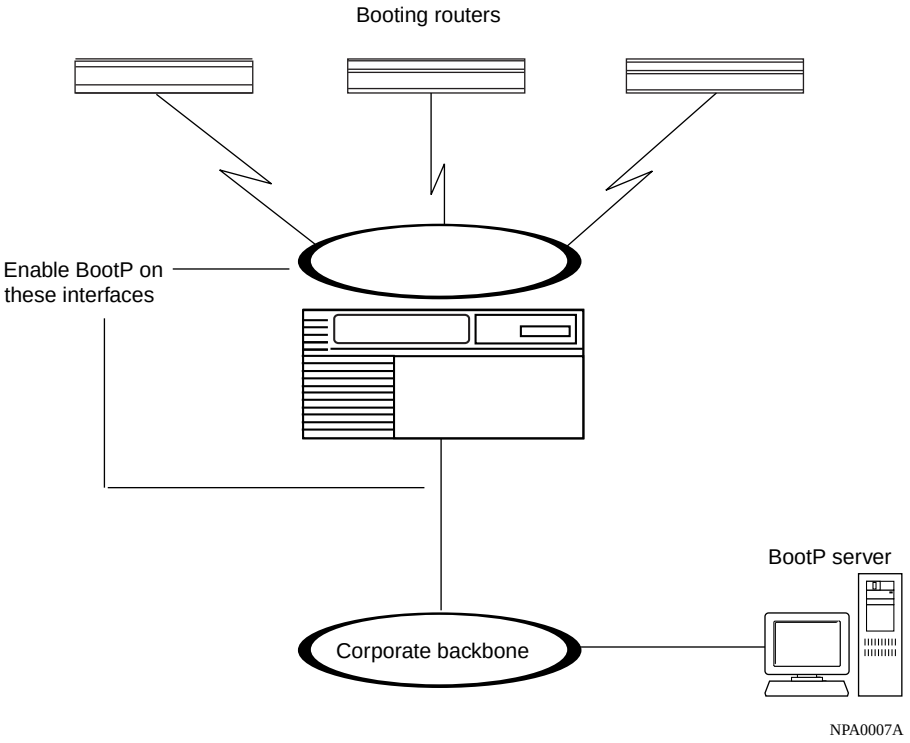

Figure 4-1. Enabling BootP in a Sample Network

To enable BootP on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the link or net module connector.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Select **BOOTP** and click on **OK**.	
6. Choose **File**.	The File menu opens.
7. Choose **Exit**.	You return to the Configuration Manager window.

Specifying Interfaces to Receive and Relay BOOTREQUEST Packets

You specify a forwarding route for BOOTREQUEST packets by defining a relationship between an interface that you want to receive BOOTREQUEST packets and another to transmit BOOTREQUEST packets. When you define this type of relationship, the interface pair appears in the BootP relay agent forwarding table.

Depending on the configuration of your network, you can specify:

- One input IP interface to forward packets to multiple output IP interfaces
- Multiple input interfaces to forward packets to multiple output interfaces
- Multiple input interfaces to forward packets to one output interface

Creating a BootP Relay Agent Forwarding Table

You must create a BootP relay agent forwarding table for every router passing BootP traffic between a router and the BootP server.

The BootP relay agent forwarding table consists of IP interfaces that you configure to receive the incoming BootP request packets and to forward the outgoing BootP request packets. The BootP relay agent forwards BootP request packets based on the IP addresses of the interfaces in this table. You can add multiple pairs of incoming and outgoing interfaces to support connections to multiple routers in your network. For more information about configuring a forwarding table, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*

Specifying the IP Interface Input/Output Address Pair

You create the BootP relay agent forwarding table by specifying the IP interface addresses (input and output) of the pair that you want to receive and forward BOOTREQUEST packets. If you enter an IP address that is not configured on the router, the notation `???` appears before the IP address (example: `??? 111.111.111.111`). After you configure the IP address on the router, Site Manager replaces `???` with the appropriate address.

Do not specify an unnumbered interface for the input or output IP interface address parameters. If you want to use an unnumbered interface to transmit BOOTREQUEST or DHCP packets to the servers, you must set up a preferred server (see "Configuring BootP Preferred Servers" on page 4-15).

To specify the IP interface input/output address pair, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Click on **Add**.	The BOOTP Addresses window opens.
7. Set the following parameters: • **Input IP Address** • **Output IP Address** Click on **Help** or see the parameter descriptions beginning on page A-19.	
8. Click on **OK**.	You return to the BOOTP Relay Agent Forwarding Table window.
9. Click on **Done**.	You return to the BOOTP Relay Agent Interface Table window.

Deleting an IP Interface Input/Output Address Pair

To delete an input/output address pair from the BootP relay agent forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Select the address pair that you want to delete.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Click on **Delete**.	The BOOTP Relay Agent Forwarding Table window no longer displays the address pair.
8. Click on **Done**.	You return to the BootP Relay Agent Interface Table window.

Disabling BootP Route Forwarding

By default, the route (interface) through which the router forwards BootP or DHCP packets to servers on the network is enabled. You can disable BootP or DHCP packet forwarding through this route.

To disable BootP route forwarding, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Select the address pair that you want to enable or disable.	
7. Set the **Enable/Disable** parameter. Click on **Help** or see the parameter description on page A-20.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Configuration Manager window.

Configuring an AN to Use EZ-Install over a Frame Relay PVC

The *upstream router* is a booting router's next-hop router. By default, when an AN router boots, the router's synchronous interfaces try to get IP addresses from the upstream router. This process is called *EZ-Install*.

If you plan to configure an AN router to use EZ-Install over a frame relay PVC in group access mode, you must create a BootP *client interface table.* You do not need to create this table if you configured the frame relay PVC to operate in direct access mode. The BootP client interface table allows you to associate the IP address of a remote AN router with the DLCI of its frame relay group access PVC.

If the upstream router's interface to the booting router is a frame relay group access PVC, you must connect to the upstream router and create a BootP client interface table (in addition to a BootP relay agent forwarding table).

For information about configuring an AN to use EZ-Install, see *Installing and Operating BayStack AN and ANH Routers*. For information about DLCIs and frame relay, see *Configuring Frame Relay Services*.

Creating a BootP Client Interface Table

You create a BootP client interface table by specifying the following:

- IP address of the remote AN router that will boot using EZ-Install over a frame relay group access PVC connection to the router.
- Frame relay PVC identification number whose destination is the remote AN that will boot using EZ-Install. Enter in decimal format the DLCI number assigned by your frame relay service provider. The frame relay network uses the DLCI number to direct data flow.

To specify a client IP address and its associated DLCI, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Client I/F**.	The BOOTP Client Interface Table window opens.
6. Click on **Add**.	The BOOTP Client Interface Address window opens.
7. Set the following parameters: • **IP Address** • **DLCI Number** Click on **Help** or see the parameter descriptions beginning on page A-21.	
8. Click on **OK**.	You return to the BOOTP Client Interface Table window.
9. Click on **Done**.	You return to the BOOTP Relay Agent Interface Table window.
10. Click on **Done**.	You return to the Configuration Manager window.

Specifying Servers for BootP Services

You can specify a forwarding route for BOOTREQUEST packets by defining a relationship between an input interface and a BootP server. By defining such a relationship, you can:

- Improve the efficiency of BOOTREQUEST packet relay.
- Transmit BOOTREQUEST packets through unnumbered output interfaces.

Configuring BootP Preferred Servers

You configure a BootP preferred server by specifying the following:

- IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients. Do not specify an unnumbered interface for this parameter.
- IP address of the server that should receive the BOOTREQUEST or DHCP packet from the relay agent.

The router can then unicast a BOOTREQUEST packet through normal IP services to that server.

To specify the relay agent IP address and the preferred BootP server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table window opens.
6. Click on **Add**.	The BOOTP Preferred Server Configuration window opens.
7. Set the following parameters: • **Relay Agent IP Address** • **Target Server IP Address** Click on **Help** or see the parameter descriptions beginning on page A-22.	
8. Click on **OK**.	You return to the BOOTP Relay Agent Preferred Server Table window.
9. Click on **Done**.	You return to the BootP Relay Agent Interface Table window.
10. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Target Server's Host Name

If you want to keep track of the names of BootP and DHCP servers, specify the target server's host name. The host name cannot exceed 63 ASCII characters, including embedded spaces.

To specify the target server's host name, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table window opens.
6. Set the **Target Name** parameter. Click on **Help** or see the parameter description on page A-23.	
7. Click on **Apply**.	
8. Click on **Done**.	You return to the BOOTP Relay Agent Interface Table window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling the Forwarding Route

By default, BootP and DHCP forwarding is enabled for the route that you configured. You can disable BootP or DHCP forwarding on this route.

To disable the forwarding route, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table window opens.
6. Set the **Enable/Disable** parameter. Click on **Help** or see the parameter description on page A-23.	
7. Click on **Apply**.	
8. Click on **Done**.	You return to the BOOTP Relay Agent Interface Table window.
9. Click on **Done**.	You return to the Configuration Manager window.

Filtering BootP and DHCP Packets

You can control whether an interface transmits BootP packets, DHCP packets, or both to a server by configuring filters for these specific packets. The default setting is BootP and allows the interface to transmit only BootP packets. Change the setting if you want to transmit DHCP messages.

To filter BootP and DHCP packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table window opens.
6. Set the **Pass Through Mode** parameter. Click on **Help** or see the parameter description on page A-23.	
7. Click on **Apply**.	
8. Click on **Done**.	You return to the BOOTP Relay Agent Interface Table window.
9. Click on **Done**.	You return to the Configuration Manager window.

Deleting the BootP Relay Agent from an IP Interface

To delete a BootP relay agent from an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on the interface from which you want to delete BootP.	
6. Click on **Delete**.	The Configuration Manager deletes the BootP relay agent and all forwarding table entries that you specified from the selected interface.
7. Click on **Done**.	You return to the Configuration Manager window.

Deleting BootP Globally

To globally delete BootP (and thereby, DHCP) from all interfaces on a router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Delete BOOTP**.	A confirmation window opens.
5. Click on **OK**.	The Configuration Manager deletes BootP from all interfaces on the router.

Chapter 5
Customizing BootP/DHCP Relay

This chapter describes how to customize BootP/DHCP relay services. It assumes that you configured an IP interface and enabled BootP/DHCP relay, as described in Chapter 1, “Starting SNMP, BootP, and DHCP Services,” and that you understand the DHCP concepts in Chapter 2, “SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts.”

Topic	Page
Setting Up the Routing Path from the DHCP Server to the Router	5-2
Deleting BootP/DHCP Relay from an IP Interface	5-4
Deleting BootP/DHCP Relay Globally	5-5

Setting Up the Routing Path from the DHCP Server to the Router

You must define a routing path between the DHCP server and the router configured as a BootP relay agent to ensure the transmission of packets from one end of the network to the other. You define this routing path by:

- Specifying interfaces to receive and forward DHCP packets
- Defining a DHCP server

Specifying Interfaces to Receive and Forward DHCP Packets

BootP/DHCP relay uses the BootP relay agent to forward packets to and receive packets from DHCP servers. You must define a forwarding route for DHCP packets by defining a relationship between an interface that receives DHCP packets from clients and an interface that sends DHCP packets to servers.

When you define this type of relationship, the interface pair appears in the BootP relay agent forwarding table. For instructions, see “Specifying Interfaces to Receive and Relay BOOTREQUEST Packets” on page 4-9.

To allow the BootP relay agent to forward DHCP packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens. This window lists all the IP interfaces that you configured for BootP services on the router.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Select the address pair that you want to configure.	
7. Set the **Pass Through Mode** parameter. Click on **Help** or see the parameter description on page A-20.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Configuration Manager window.

Defining DHCP Servers

If DHCP clients obtain IP addresses and other configuration information from a DHCP server on a different subnet, connected through a router, then you must define a DHCP preferred server by specifying the IP address of the BootP relay agent on the local router and the IP address of the target server. The router can then unicast a DHCP packet through normal IP services to that server. For instructions, see “Specifying Servers for BootP Services” on page 4-14.

To allow DHCP operation, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Pref Serv**.	The BOOTP Relay Agent Preferred Server Table window opens.
6. Set the **Pass Through Mode** parameter. Click on **Help** or see the parameter description on page A-23.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Click on **Apply**.	
8. Click on **Done**.	You return to the Configuration Manager window.

Deleting BootP/DHCP Relay from an IP Interface

To delete BootP/DHCP relay from an IP interface, while maintaining BootP on that interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Click on **Forward I/F**.	The BOOTP Relay Agent Forwarding Table window opens.
6. Select the address pair from which you want to delete BootP/DHCP forwarding.	
7. Set the **Pass Through Mode** parameter to **BOOTP**. Click on **Help** or see the parameter description on page A-23.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Configuration Manager window.

To delete both BootP/DHCP relay and BootP from an IP interface, delete the BootP relay agent on that interface. For instructions, see “Deleting the BootP Relay Agent from an IP Interface” on page 4-18.

Deleting BootP/DHCP Relay Globally

To delete BootP/DHCP globally, you must delete BootP globally. For instructions, see “Deleting BootP Globally” on page 4-19.

Chapter 6
Customizing the DHCP Server

This chapter describes how to customize the DHCP server configuration on the router. It assumes that you configured an IP interface and enabled a DHCP server on the interface, as described in Chapter 1, “Starting SNMP, BootP, and DHCP Services,” and that you understand the DHCP server concepts in Chapter 2, “SNMP, BootP, BootP/DHCP Relay, and DHCP Server Concepts.”

Topic	Page
Modifying the DHCP Server Configuration	6-2
Disabling and Reenabling the DHCP Server	6-8
Deleting the DHCP Server from the Router	6-9
Deleting DHCP Globally	6-9

Modifying the DHCP Server Configuration

You can determine how a DHCP server functions on the router by modifying its configuration. Use the sections in this chapter as a guide.

Configuring the NetID Server Manager IP Address

You must configure the IP address of the NetID Server Manager to allow it to communicate with the target DHCP server on the router. To configure the IP address of the NetID Server Manager, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Server Manager IP Address** parameter. Click on Help or see the parameter description on page A-24.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the DHCP Server IP Address

To ensure that the DHCP server on the router can communicate with the NetID Server Manager, you must specify a local IP address that the DHCP server can use to identify itself to the NetID Server Manager. This address must correspond to the address of an actual local IP interface configured on the router. This address cannot be a circuitless IP address.

To specify a local IP address for the DHCP server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Local IP Address** parameter. Click on **Help** or see the parameter description on page A-27.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the DHCP Server TCP Port Number

To allow the DHCP server to communicate with the NetID Server Manager using TCP, you must specify a remote TCP port number on the DHCP server. This number must match the port number that you specify on the NetID Server Manager.

You specify the TCP port number on the NetID Server Manager when you install the NetID Server Manager software. The default TCP port number is 24736. For information about specifying a remote port number for the NetID Server Manager, see the *NetID System Administrator's Guide*.

To specify the TCP port number on the DHCP server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **DHCP Server TCP Port Number** parameter. Click on **Help** or see the parameter description on page A-24.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring the Number of Pings and the Ping Timeout

Before the DHCP server on the router assigns an IP address to a DHCP client, it must ensure that the IP address is not already in use on the network. To verify that the IP address is available, the DHCP server sends out an ICMP echo request, called a *ping*.

- If the server fails to receive a response to the request within the specified timeout period (ping request timeout), the DHCP server offers the IP address and grants a lease to the client.
- If the DHCP server receives a response to the request, the IP address is unavailable and therefore cannot be offered to the client.

By default, the DHCP server pings the IP address for a prospective DHCP client only once before declaring it available.

By default, the DHCP server waits 750 milliseconds (that is, 0.75 second) for a conflict detection ping to time out before determining that an IP address is available to assign to a client. If you want to change the length of time that the DHCP server waits, specify a value from 1 through 5000 milliseconds (5 seconds).

Note: Typically, DHCP clients retransmit a DHCPDISCOVER message after 2 seconds. Thus, if you specify a ping timeout value greater than 2000 milliseconds (2 seconds), the router may transmit spurious messages. The same consideration applies if you set the values of the ping timeout and the number of pings so that their product (timeout value times the number of pings) is greater than 2000.

To specify the number of times that the DHCP server pings the IP address of a prospective DHCP client or to specify the ping timeout value, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the following parameters: • **Number of Pings** • **Ping Timeout** Click on **Help** or see the parameter descriptions beginning on page A-25.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the DHCP Server Operating Mode

By default, the mode in which the DHCP server operates is called *safe mode*.

When safe mode is enabled, the DHCP server cannot acknowledge the DHCP client's lease request until it receives a successful lease-commit acknowledgment from the NetID Server Manager. Typically, you enable safe mode when you want to ensure that the client receives only successful committed leases from the DHCP server and the NetID Server Manager.

When safe mode is disabled, the DHCP server immediately returns a lease-granted acknowledgment to the DHCP client in response to its lease request without waiting for a successful lease-commit acknowledgment from the NetID Server Manager. With safe mode disabled, the DHCP server can still assign IP addresses to clients even if it loses communication with the NetID Server Manager.

To enable or disable safe mode on the DHCP server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Safe Mode** parameter. Click on **Help** or see the parameter description on page A-26.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Pending Leases

By default, the maximum number of lease requests sent to the DHCP server that are pending commitment by the NetID Server Manager is 2. You can increase the maximum number of pending leases by specifying a value from 1 through 255.

When the number of lease requests sent to the NetID Server Manager and pending commitment by the NetID Server Manager reaches the configured value, the DHCP server holds all subsequent lease requests. When the number of pending requests decreases to half this value, the DHCP server begins forwarding requests to the NetID Server Manager again.

To specify the maximum number of lease requests sent to the DHCP server that are pending commitment, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Max. No. Pending Leases** parameter. Click on **Help** or see the parameter description on page A-26.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Debug Level

By default, only debug messages with a debug level of 0 are written to the log file for the DHCP server. You can change the debug messaging level for the DHCP server by entering a value from 1 through 10.

Specifying a higher debug level causes additional messages to appear in the log file. Because additional information can rapidly fill the log file and cause loss of other information, change the debug level only to resolve critical problems.

To specify the debug messaging level for the DHCP server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Debug Level** parameter. Click on Help or see the parameter description on page A-27.	
6. Click on **OK**.	You return to the Configuration Manager window.

Disabling and Reenabling the DHCP Server

After you create the DHCP server on the router as described in Chapter 1, "Starting SNMP, BootP, and DHCP Services," you can disable or reenable it on an interface or globally. If you disable DHCP for the router, it is no longer available on any IP circuit.

To disable or reenable the DHCP server on an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **BOOTP**.	The BOOTP menu opens.
4. Choose **Relay Agent Interface Table**.	The BOOTP Relay Agent Interface Table window opens.
5. Set the **DHCP Server Enable** parameter**.** Click on **Help** or see the parameter description on page A-18.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

To disable or reenable the DHCP server on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Global.**	The DHCP Global Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-24.	
6. Click on **OK**.	You return to the Configuration Manager window.

Deleting the DHCP Server from the Router

To delete the DHCP server from the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DHCP**.	The DHCP menu opens.
4. Choose **Delete DHCP.**	A confirmation window opens.
5. Click on **OK**.	Site Manager deletes the DHCP server from the router.

Deleting DHCP Globally

To delete DHCP globally, you must delete BootP globally. For instructions, see “Deleting BootP Globally” on page 4-19.

Appendix A
Site Manager Parameter Descriptions

This appendix contains the Site Manager parameter descriptions for SNMP, BootP, BootP/DHCP relay, and DHCP server services. You can display the same information using the Help button in Site Manager.

This appendix contains the following information:

Topic	Page
SNMP Global Parameters	A-3
SNMP Community Parameters	A-5
SNMP Manager Parameters	A-6
SNMP Trap Exception Parameters	A-7
SNMP Threshold Global Parameters	A-8
SNMP Threshold Interface Parameters	A-9
BootP and DHCP Parameters	A-16

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

SNMP Global Parameters

Use the following guidelines to configure SNMP global parameters in the Configuration Manager window.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: Enable

Options: Enable | Disable

Function: Specifies the state of the SNMP agent on all interfaces that support IP.

Instructions: Select Enable to enable the SNMP agent; select Disable to disable the SNMP agent.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.1

Parameter: Use Lock

Path: Configuration Manager > Protocols > IP > SNMP > Global

Default: Enable

Options: Enable | Disable

Function: Specifies whether the agent responds to multiple network management stations issuing simultaneous SNMP **set** commands to the router. When you set this parameter to Enable, the agent identifies the station from which it receives the next SNMP **set** command and, for a time equal to the value of the Lock Time Out parameter, responds only to SNMP **set** commands from that station. If the agent receives an SNMP **set** command from another network management station during this time, it issues an SNMP genErr GetResponse PDU, which that station logs as an SNMP set error message.

Instructions: Select Enable to prohibit the agent from responding to simultaneous SNMP commands from multiple network management stations.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.2

Parameter:	**Lock TimeOut**
Path:	Configuration Manager > Protocols > IP > SNMP > Global
Default:	2 (minutes)
Options:	1 to 60 (minutes)
Function:	Specifies the maximum number of minutes that the agent allows an idle network management station to hold a lock on it. During this time, the agent locks out SNMP **set** commands from other network management stations. The lock timer is reset each time the locking manager issues an SNMP **set** command.
Instructions:	Enter the number of minutes only if you set the Use Lock parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.4

Parameter:	**Authentication Failure Traps**
Path:	Configuration Manager > Protocols > IP > SNMP > Global
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the router attempts to generate an authentication failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.
Instructions:	Select Enable to enable the router to generate authentication failure traps. If you select Enable, you must configure an SNMP manager to receive the trap. You configure a trap in the Trap Configuration window. Select Disable to prohibit the router from generating authentication failure traps.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.3.5

SNMP Community Parameters

Use the following guidelines to configure SNMP community parameters in the SNMP Community window.

Parameter: Community Name

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Add Community | Edit Community

Default: None

Options: Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces

Function: Specifies the name of the SNMP community.

Instructions: Enter the SNMP community name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.2.1.3

Parameter: Access

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Add Community | Edit Community

Default: Read Only

Options: Read Only | Read-Write

Function: Specifies the access privileges that the router grants to all members of this SNMP community.

Instructions: Select Read Only to allow members of this community to view configuration and performance information about this router.

Select Read-Write to allow members of this community to not only view configuration and performance information about this router, but also to change the router's configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.2.1.4

SNMP Manager Parameters

Use the following guidelines to configure SNMP manager parameters in the SNMP Manager window.

Parameter: Trap Port

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Managers > Manager > Edit Manager

Default: 162

Options: 1 to 9999

Function: Specifies the number of the UDP port on the management station to which the agent sends traps.

Instructions: The standard port number for trap messages is 162; however, you can enter a different port number. Be sure not to specify a port that another application uses.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.3.1.5

Parameter: Trap Types

Path: Configuration Manager > Protocols > IP > SNMP > Communities > Community > Managers > Manager > Edit Manager

Default: Generic

Options: None │ Generic │ Specific │ All

Function: Specifies the type of trap that the agent sends to this manager.

Instructions: Select None to prohibit the agent from sending traps to this manager.

Select Generic to configure the agent to send the well-defined SNMP traps (cold-start, warm-start, and authentication failure traps) to the manager. The cold-start and warm-start traps are automatically active in the SNMP agent; however, you must enable the Authentication Failure Traps global parameter for the agent to send such traps to this manager.

Select Specific to configure the agent software to send all enabled log event traps to this manager.

Select All to send cold-start traps, warm-start traps, and all enabled log event traps to this manager.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.3.1.6

SNMP Trap Exception Parameters

Use the following guidelines to configure SNMP trap exception parameters in the Add Trap window.

Parameter: Entity Code

Path: Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**

Default: None

Options: Any valid entity code

Function: Specifies the entity code for the event for which you want to configure an exception.

Instructions: Enter the entity code for the event for which you want to configure an exception. For entity codes, see the event database.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.3

Parameter: Event Code

Path: Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**

Default: None

Options: Any valid event code number

Function: Specifies the code number for the event for which you want to configure an exception.

Instructions: Enter the event code number for the event for which you want to configure an exception. For event codes, see the event database.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.4

Parameter:	**Always/Never Trap**
Path:	Configuration Manager > Protocols > IP > SNMP > Trap Configuration > Exceptions > **Add**
Default:	None
Options:	Always | Never
Function:	Specifies whether the SNMP agent always sends or never sends this trap to the network management station. The instructions that you specify in this field override the settings in the Trap Configuration window, and affect traps sent from every slot in the router.
Instructions:	Select Always or Never.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.6.1.2

SNMP Threshold Global Parameters

Use the following guidelines to configure SNMP threshold global parameters in the Edit Thresholds Global Parameters window.

Parameter:	**Enable/Disable**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Global
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the threshold feature on a router.
Instructions:	Select Enable to enable thresholds. Select Disable to disable thresholds.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.1.1

Parameter: **Polling Interval**

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Global

Default: 60 (seconds)

Options: 5 seconds minimum; no maximum value

Function: Sets the time interval at which the agent polls the variable to determine whether that variable has reached a threshold.

Instructions: Specify the number of seconds for the polling interval. Remember that the more often the agent polls the variable, the more memory it needs to manage the thresholds for this statistic.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.1.2

SNMP Threshold Interface Parameters

Use the following guidelines to configure SNMP threshold interface parameters in the Thresholds Interface Lists window.

Parameter: **Threshold Enable**

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Enable

Options: Enable | Disable

Function: Turns the threshold for this variable on and off.

Instructions: Select Enable if you want the agent to apply the threshold to this variable.

Select Disable if you want the agent to ignore the threshold for this variable.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.2

Parameter:	**Threshold Low Value**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	0
Options:	Any integer value
Function:	Sets the value of the low threshold for this variable.
Instructions:	Specify the level at which you want the agent to generate a low-threshold exception event.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.5

Parameter:	**Threshold Low Event Level**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level of the event message that the agent generates when a variable exceeds the low threshold.
Instructions:	Select Info if you want low-threshold exceptions to generate routine events that require no action. Select Warning if you want low-threshold exceptions to generate events that indicate that an unexpected situation occurred. Select Debug if you want low-threshold exceptions to generate events that you can use to solve network problems.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.6

Parameter: Threshold Medium Value

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 0

Options: Any integer value

Function: Sets the value of the medium threshold for this variable.

Instructions: Specify the level at which you want the agent to generate a medium-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.7

Parameter: Threshold Medium Event Level

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level of the event message that the agent generates when a variable exceeds the medium threshold.

Instructions: Select Info if you want medium-threshold exceptions to generate routine events that require no action.

Select Warning if you want medium-threshold exceptions to generate events that indicate that an unexpected situation occurred.

Select Debug if you want medium-threshold exceptions to generate events that you can use to solve network problems.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.8

Parameter:	**Threshold High Value**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	0
Options:	Any integer value
Function:	Sets the value of the high threshold for this variable.
Instructions:	Specify the level at which you want the agent to generate a high-threshold exception event.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.9

Parameter:	**Threshold High Event Level**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level of the event message that the agent generates when a variable exceeds the high threshold.
Instructions:	Select Info if you want high-threshold exceptions to generate routine events that require no action. Select Warning if you want high-threshold exceptions to generate events that indicate that an unexpected situation occurred. Select Debug if you want high-threshold exceptions to generate events that you can use to solve network problems.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.10

Parameter: Threshold Units

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Persecond

Options: Persecond | Absolute

Function: Specifies the units used to determine whether a variable has exceeded a threshold.

Instructions: Select Persecond if you want the agent to generate a threshold event when the variable's rate of change *per second* reaches a threshold.

Select Absolute if you want the agent to generate a threshold event when the value of the variable reaches a threshold.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.12

Parameter: Threshold Action

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: Greaterthan

Options: Greaterthan | Lessthan

Function: Specifies when the agent generates a threshold event.

Instructions: Select Greaterthan if you want to record threshold events when the value of the variable is *greater than* the threshold specified.

Select Lessthan if you want to record threshold events when the value of the variable is *less than* the threshold specified.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.13

Parameter: Threshold Max Successive Alarms

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 5

Options: 1 to 20

Function: Specifies the maximum number of successive alarms that the agent generates for this variable. A successive alarm represents two or more polling periods when the agent generates an alarm as a result of an exception at the same threshold level.

Instructions: Specify the maximum number of successive alarms. When the agent exceeds the maximum number of alarms, it marks the threshold as held. The agent generates no more alarms until the variable either crosses the threshold at a different level or crosses no threshold for the number of polling intervals equal to the value of the Threshold HoldDown Intervals parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.14

Parameter: Threshold HoldDown Intervals

Path: Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds

Default: 1

Options: 1 to 20

Function: Specifies the number of exception-free polling intervals through which a variable in a held state must pass before the variable is no longer considered held.

Instructions: Specify the number of exception-free polling intervals. The lower the number that you select, the more likely the agent is to generate repetitive event messages for a variable that is intermittently exceeding thresholds.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.15

Parameter:	**Threshold Label**
Path:	Configuration Manager > Protocols > Global Protocols > Thresholds > Thresholds
Default:	ASN.1 OID
Options:	ASN.1 OID | String identifier
Function:	Specifies a name for the MIB object in string format to replace the ASN.1 object identifier. The string that you enter appears in the log file, making it easier to identify the object that is the subject of the trap.
Instructions:	Type a name for the MIB object, or leave this field empty to use the ASN.1 object identifier.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.22

BootP and DHCP Parameters

This section describes the parameters you use to configure BootP/DHCP relay for your router.

BootP Relay Agent Interface Parameters

Use the following guidelines to configure BootP and DHCP parameters in the BOOTP Relay Agent Interface Table window.

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: Enable

Options: Enable | Disable

Function: Specifies whether BootP is active on the network interface.

Instructions: Select Enable to enable BootP on the network interface. Select Disable to disable BootP on the network interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.2

Parameter: Hops

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 4

Options: 1 to 16

Function: Specifies the maximum number of hops from the client to the server. A hop is the logical distance between two devices. If the value in the hops field of a BOOTREQUEST packet is greater than the number that you specify for this parameter, the router drops the packet.

Instructions: Accept the default of 4 hops or specify a number from 1 through 16.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.5

Parameter: Timeout Secs.

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 0

Options: 0 to 65535

Function: Specifies the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the seconds field of a BOOTREQUEST packet is less than the value that you specify for this parameter, the router drops the packet.

Instructions: Accept the default, 0, or specify a number from 1 through 65535 (equal to 18 hours, 12 minutes, and 15 seconds).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.6

Parameter: Pass Through Mode

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: BOOTP

Options: BOOTP | DHCP | BOOTP/DHCP

Function: Specifies whether the interface relays BootP, DHCP, or both BootP and DHCP requests.

Instructions: Select BOOTP to relay BootP requests. Select DHCP to relay DHCP requests. Select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.16

Parameter: Interface Priority

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: 0

Options: 0 to 16

Function: Indicates the priority of the interface on a multinetted interface.

Instructions: Enter an integer from 1 through 16 to indicate the priority of the interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.20

Parameter: DHCP Server Enable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: Disable

Options: Enable │ Disable

Function: Specifies whether the DHCP server is enabled or disabled on this network interface.

Instructions: Select Enable to enable the DHCP server on the network interface. Select Disable to disable the DHCP server on the network interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.21

Parameter: ARP Cache Enable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table

Default: Disable

Options: Enable │ Disable

Function: Enables and disables the BootP ARP cache entry feature. This feature allows devices that do not run ARP to use the BootP relay agent on the router. This parameter has no effect on the operation of DHCP.

Instructions: If you want the BootP relay agent to add or update an ARP entry for a client based on the information provided in a BootP reply message, choose Enable. Otherwise, choose Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.23

BootP Address Parameters

Use the following guidelines to configure BootP and DHCP parameters in the BOOTP Addresses window.

Parameter: Input IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives BOOTREQUEST packets from clients.

Instructions: Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, then configure this IP address on the router, if you have not already done so.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter: Output IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F > Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that forwards BOOTREQUEST packets to an external network.

Instructions: Enter the IP address of a numbered network interface that you want to send BOOTREQUEST or DHCP packets to servers, and then configure this IP address on the router, if you have not already done so.

Do not specify an unnumbered interface for this parameter. If you want to use an unnumbered interface to send BOOTREQUEST or DHCP packets to servers, you must set up a preferred server.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

Parameter:	**Enable/Disable**
Path:	Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this forwarding route is active.
Instructions:	Select Enable to allow BootP or DHCP forwarding through this route. Select Disable to prevent BootP or DHCP forwarding through this route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.2

Parameter:	**Pass Through Mode**
Path:	Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Forward I/F**
Default:	BOOTP
Options:	BOOTP | DHCP | BOOTP/DHCP
Function:	Specifies whether the interface relays BootP, DHCP, or both BootP and DHCP requests.
Instructions:	Select BOOTP to relay BootP requests. Select DHCP to relay DHCP requests. Select BOOTP and DHCP to relay both kinds of requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.5

BootP Client Interface Address Parameters

Use the following guidelines to configure BootP and DHCP parameters in the BOOTP Client Interface window.

Parameter: IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Client I/F** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP address of the remote AN that will boot using EZ-Install over a frame relay group access PVC connection to the router.

Instructions: Enter the IP address of the remote AN.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.1.1.1.3

Parameter: DLCI Number

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Client I/F > Add**

Default: None

Options: 16 to 1007

Function: Specifies the frame relay PVC identification number whose destination is the remote AN that will boot using EZ-Install. The frame relay network uses the DLCI number to direct data flow.

Instructions: Enter the DLCI number, in decimal format, for the group access PVC to the remote AN. Use the DLCI number assigned by your frame relay service provider.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.1.1.1.2

BootP Preferred Server Configuration Parameters

Use the following guidelines to configure BootP and DHCP preferred server configuration parameters.

Parameter: Relay Agent IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the IP interface that receives BOOTREQUEST or DHCP packets from clients.

Instructions: Enter the IP address of a numbered network interface that you want to receive BOOTREQUEST or DHCP packets from clients, and then configure this IP address on the router, if you have not already done so.

Do not specify an unnumbered interface for this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.3

Parameter: Target Server IP Address

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv** > **Add**

Default: None

Options: Any valid IP address

Function: Specifies the address of a server that should receive BOOTREQUEST or DHCP packets.

Instructions: Enter the IP address of the server that should receive the BOOTREQUEST or DHCP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.4

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv**

Default: Enable

Options: Enable │ Disable

Function: Specifies whether the forwarding route is active.

Instructions: Select Enable to allow BootP or DHCP forwarding through this route. Select Disable to prevent BootP or DHCP forwarding through this route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.2

Parameter: Target Name

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv**

Default: None

Options: Any string of printable ASCII characters, up to 63 characters in length, including embedded spaces

Function: Specifies the target server's host name.

Instructions: If you want to keep track of the names of BootP or DHCP servers, enter the target server's host name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.5

Parameter: Pass Through Mode

Path: Configuration Manager > Protocols > IP > BOOTP > Relay Agent Interface Table > **Pref Serv**

Default: BOOTP

Options: BOOTP │ DHCP │ BOOTP/DHCP

Function: Specifies whether the interface relays BootP, DHCP, or both BootP and DHCP requests to the target server.

Instructions: Select BOOTP to relay BootP requests. Select DHCP to relay DHCP requests. Select BOOTP and DHCP to relay both kinds of requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.3.1.6

DHCP Server Global Parameters

Use the following guidelines to configure DHCP server global parameters in the DHCP Global Parameters window.

Parameter: Enable

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global
Default: Enable
Options: Disable | Enable
Function: Specifies whether the DHCP server is enabled or disabled on the router.
Instructions: Select Enable to enable the DHCP server on the router. Select Disable to disable the DHCP server on the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.2

Parameter: Server Manager IP Address

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global
Default: None
Options: Any valid IP address
Function: Specifies the IP address of the NetID Server Manager that provides and manages DHCP lease information for this DHCP server.
Instructions: Enter the IP address of the NetID DHCP Server Manager.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.3

Parameter: DHCP Server TCP Port Number

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global
Default: None
Options: A valid TCP port number
Function: Specifies the remote port number over which the DHCP server on the router communicates with the NetID Server Manager.
Instructions: Enter a remote port number on the DHCP server that matches the port number for the NetID Server Manager. For information about specifying a remote port number for the NetID Server Manager, see the *NetID System Administrator's Guide*.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.4

Parameter: Number of Pings

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global

Default: 1

Options: 1 to 9999

Function: Specifies the number of ping attempts that the DHCP server makes to the IP address of the prospective DHCP client to detect possible conflicts before declaring the client address available.

Instructions: Accept the default, 1, or specify a number from 1 through 9999 to determine the number of ping attempts that the DCHP server makes to the prospective DHCP client IP address. Normally, a DHCP server makes only one ping attempt.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.5

Parameter: Ping Timeout

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global

Default: 750

Options: 1 to 5000

Function: Specifies the amount of time (in milliseconds) that the DHCP server waits for a conflict detection ping to time out.

Instructions: Accept the default, 750 milliseconds (0.75 second), or specify a value from 1 through 5000. Typically, DHCP clients retransmit a DHCPDISCOVER message after 2 seconds. Thus, if you specify a ping timeout value greater than 2000 milliseconds (2 seconds), the router may transmit spurious messages. The same consideration applies if you set the values of the ping timeout and the number of pings so that their product (timeout value times the number of pings) is greater than 2000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.6

Parameter: Safe Mode

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global

Default: Enable

Options: Enable │ Disable

Function: Specifies whether the DHCP server waits until the NetID Server Manager acknowledges receipt of a successful lease commitment before sending a lease-granted acknowledgment to the DHCP client.

Instructions: Select Enable if you want the DHCP server to wait for the NetID Server Manager to confirm receipt of the successful lease commitment. Select Disable if you want the DHCP server to immediately send back a lease-granted acknowledgment to the DHCP client without waiting for a commit-succeeded acknowledgment from the NetID Server Manager.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.7

Parameter: Max. No. Pending Leases

Path: Configuration Manager > Protocols > Global Protocols > DHCP > Global

Default: 2

Options: 1 to 255

Function: Specifies the maximum number of lease requests sent to the DHCP server that are pending commitment by the NetID Server Manager. When the number of lease requests sent to the NetID Server Manager and pending commitment by the NetID Server Manager reaches this value, the DHCP server holds all subsequent lease requests until the number of requests pending decreases to half this value. Then the DHCP server begins transmitting requests to the NetID Server Manager again.

Instructions: Accept the default, 2, or specify a number from 1 through 255.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.24.1.1.8

Parameter: Debug Level

Path:	Configuration Manager > Protocols > Global Protocols > DHCP > Global
Default:	0
Options:	1 to 10
Function:	Specifies the debug level messaging that you want to display in the log file for the DHCP server. Normally, only debug messages with a debug level of 0 are written to the log file.
Instructions:	Specify the debug messaging level. Specifying a higher debug level causes additional messages to appear in the log file. Because additional information can rapidly fill the log file and cause loss of other information, change the debug level only to resolve critical problems.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.24.1.1.9

Parameter: Local IP Address

Path:	Configuration Manager > Protocols > Global Protocols > DHCP > Global
Default:	0.0.0.0
Options:	Valid IP address
Function:	Specifies the IP address that the DHCP server uses to identify itself to the NetID Server Manager serving this DHCP server.
Instructions:	Enter the IP address of the DHCP server. This address must correspond to the address of an actual local interface configured on the router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.24.1.1.10

Appendix B
SNMP show Commands

To display configuration and statistical information about SNMP from the management information base (MIB), use the BCC **show snmp** command.

This appendix includes descriptions of the following **show** commands:

Command	Page
show snmp community	B-2
show snmp stats	B-3
show snmp trap-entity	B-4
show snmp trap-event	B-5

show snmp community

The **show snmp community** command displays information about SNMP communities configured on the router. An SNMP community is a logical relationship between the SNMP agent on the router and one or more SNMP managers.

The output includes the following information:

SNMP Management Communities	
Index	Unique numeric value that has a one-to-one correspondence with the community name.
Community Name	Name of the community.
Community Access	Access privileges that the router grants to all members of this community, as follows: • *Read* -- All members of this community can only view configuration and performance information about this router. • *Read/Write* -- All members of this community can both view configuration and performance information about this router and change the router's configuration.
SNMP Manager Information	
Manager Address	IP address of this manager.
Manager Name	Name of this manager.
Trap Port	UDP port on which this manager is listening for traps.
Trap Type	Valid trap types to be sent to the manager, as follows: • *None* -- Prohibits the agent software from transmitting traps to this manager. • *Generic* -- Lets the agent software transmit the well-defined SNMP traps (coldStart, warmStart, egpNeighborLoss, linkUp, linkDown, authenticationFailure, and enterpriseSpecific) to the manager. • *Specific* -- Lets the agent software transmit all enabled log event traps to this manager. • *All* -- Transmits both generic and specific trap types to this manager.
Community Name	Name of the community.

show snmp stats

The **show snmp stats** command displays statistics about the protocol data units (PDUs) received and forwarded by SNMP. The output includes the following information:

Authentication Type	Authentication type for the area: None or Simple Password.
Received PDUs	Total number of PDUs received by SNMP from the transport entity.
Transmitted PDUs	Total number of PDUs sent by SNMP to the transport entity.
MIB Objects Retrieved	Total number of MIB objects retrieved successfully by the agent.
MIB Objects Set	Total number of MIB objects that have been set successfully.
Get Request PDUs Accepted and Processed	Total number of Get-Request PDUs accepted and processed.
Get Next Request PDUs Accepted and Processed	Total number of GetNext-Request PDUs accepted and processed.
Get Response PDUs Generated	Total number of GetResponse PDUs accepted and processed.
Set Request PDUs Accepted and Processed	Total number of Set-Request PDUs accepted and processed.
Trap PDUs Generated	Total number of Trap PDUs accepted and processed.
Decoding ASN.1 Parsing Errors	Total number of ASN.1 parsing errors during decoding.
Received Bad Community Name PDUs	Total number of PDUs that had an invalid community string.
Received Unsupported Operation PDUs	Total number of PDUs requesting an operation unsupported by the community.
Generated PDUs with tooBig Error	Total number of PDUs delivered with an error status designated as “tooBig.”
Generated PDUs with noSuchName Error	Total number of PDUs delivered with an error status designated as “noSuchName.”
Generated PDUs with badValue Error	Total number of PDUs delivered with an error status designated as “badValue.”

(continued)

Generated PDUs with readOnly Error	Total number of PDUs delivered with an error status designated as “readOnly.”
Generated PDUs with genErr Error	Total number of PDUs delivered with an error status designated as “genErr.”

show snmp trap-entity

The **show snmp trap-entity** command displays information about traps generated on the router. The output includes the following information:

Entity Name	Name of this entity on the router.
Entity Number	Number of this entity on the router.
Slot Number	Number of the slot where this entity is configured.
State	Operating state of this entity: enabled or disabled.
Fault Message	Attribute that controls the entity’s fault messages: • *On* -- The router generates this trap whenever a fault event occurs for this entity and slot number. • *Off* -- The router does *not* generate this trap whenever a fault event occurs for this entity and slot number.
Warning Message	Attribute that controls the entity’s warning messages: • *On* -- The router generates this trap whenever a warning event occurs for this entity and slot number. • *Off* -- The router does *not* generate this trap whenever a warning event occurs for this entity and slot number.
Info Message	Attribute that controls the entity’s info messages: • *On* -- The router generates this trap whenever an info event occurs for this entity and slot number. • *Off* -- The router does *not* generate this trap whenever an info event occurs for this entity and slot number.
Trace Message	Attribute that controls the entity’s trace messages: • *On* -- The router generates this trap whenever a trace event occurs for this entity and slot number. • *Off* -- The router does *not* generate this trap whenever a trace event occurs for this entity and slot number.
Debug Message	Attribute that controls the entity’s debug messages: • *On* -- The router generates this trap whenever a debug event occurs for this entity and slot number. • *Off* -- The router does *not* generate this trap whenever a debug event occurs for this entity and slot number.

show snmp trap-event

The **show snmp trap-event** command displays the events configured as SNMP traps. The output includes the following information:

Event Name	Name of the software module reporting the event.
Event Entity	Number of the software module reporting the event.
Event Number	Number of the slot on which the event occurred.
State	Configured state of the trap: enabled or disabled.

Index

A

access control, SNMP view-based
  communities
    configuring, 3-23
    deleting, 3-24
    listing information for, 3-23
  views
    associating with a community, 3-23
    configuring, 3-19
    deleting, 3-22
    deleting contents, 3-22
    disassociating from communities, 3-24
    listing, 3-21
    listing contents, 3-21

Access parameter (SNMP community), 3-11, A-5

access, restricting on SNMP router, 1-5

acronyms, xvii

agents, BootP relay
  customizing, 4-2
  description, 2-11
  forwarding table, specifying interfaces for, 4-9
  passing packets to DHCP servers, 2-20

agents, SNMP, 2-2

Always/Never Trap parameter (SNMP trap exception), 3-30, A-8

AN router, configuring BootP for connection to frame relay PVC, 4-13

ARP Cache Enable parameter (BootP/DHCP relay agent interface), 4-3, A-18

ARP cache support, 4-3

Authentication Failure Traps parameter (SNMP global), 3-8, A-4

B

BootP
  AN router, configuring for connection to frame relay PVC, 4-13
  client interface table, creating, 4-13
  customizing
    BootP/DHCP relay, 5-1
    relay agent, 4-2
  deleting
    globally, 4-19
    relay from an IP interface, 4-18
  description, 2-10
  disabling, 4-2
  enabling, 4-2, 4-7
  forwarding table, specifying interfaces for, 4-9
  hops, specifying maximum number of, 4-4
  packet relay, 2-12
  packets, filtering, 4-17
  preferred servers, configuring, 4-15
  reenabling, 4-2
  relay mode, specifying, 4-6
  route forwarding, 4-12
  routing paths between BootP server and router, 4-7
  servers, configuring preferred, 4-15
  starting, 1-6
  timeout, specifying minimum, 4-4

BootP/DHCP relay. *See* DHCP

Bootstrap Protocol. *See* BootP

C

communities, SNMP
  access privileges
    description, 2-4
    specifying, 3-10
  adding, 3-9, 3-22

communities, SNMP *(continued)*
agent views, 2-5
deleting, 3-12
description, 2-4
managers, configuring, 3-13
name, specifying, 3-9
Community Name parameter (SNMP community), 3-10, A-5
configuring
BootP
preferred servers, 4-15
relay agent, 4-2
routing path between BootP server and router, 4-7
DHCP server, 6-2
IP for global protocols, 1-2
SNMP
community managers, 3-13
global parameters, 3-3
thresholds, 3-31
trap exceptions, 3-28
traps, 3-25
view-based access control, 3-19
conventions, text, xvi
customer support, xix
customizing
BootP, 4-1
BootP/DHCP relay, 5-1
DHCP server, 6-1
SNMP, 3-1

D

Debug Level parameter (DHCP server), 6-7, A-27
deleting
BootP
globally, 4-19
relay from IP interface, 4-18
BootP/DHCP
globally, 5-5
relay from an IP interface, 5-4
DHCP
globally, 4-19, 6-9
server from the router, 6-9
SNMP
communities, 3-12
managers, 3-17
trap exceptions, 3-30
view contents, 3-22
views, 3-22
DHCP
client, description, 2-16
customizing BootP/DHCP relay, 5-1
deleting
globally, 4-19, 6-9
relay from an IP interface, 5-4
description, 2-14
enabling on an interface, 1-7
hops, specifying maximum number of, 4-4
interoperability with BootP, 2-14
packet, description, 2-19
preferred servers, specifying, 5-3
relay mode, specifying, 4-6
servers, specifying preferred, 5-3
timeout, specifying minimum, 4-4
See also BootP
DHCP server
customizing, 6-1
deleting, 6-9
description, 2-16
disabling, 6-8
enabling, 1-8
host name, configuring, 4-16
interoperability with BootP clients, 2-14
IP address, specifying for communication with NetID Server Manager, 6-2
NetID Server Manager
description, 2-16
IP address for communication with DHCP server, specifying, 6-2
operating mode, 6-5
pending leases, specifying number of, 6-6
ping timeout, specifying, 6-4
reenabling, 6-8
starting, 1-8
TCP port number, specifying, 6-3
timeout, specifying ping, 6-4
DHCP Server Enable parameter (BootP/DHCP relay agent interface), 1-9, 6-8, A-18

DHCP Server TCP Port Number parameter (DHCP server), 6-4, A-24
DLCI Number parameter (BootP/DHCP client interface address), 4-14, A-21

E

Enable parameter
DHCP server, 6-9, A-24
SNMP global, 3-4, A-3
Enable/Disable parameter
BootP/DHCP address, 4-12, A-20
BootP/DHCP preferred server, 4-17, A-23
BootP/DHCP relay agent interface, 4-2, A-16
SNMP threshold global, 3-32, A-8
Entity Code parameter (SNMP trap exception), 3-30, A-7
Event Code parameter (SNMP trap exception), 3-30, A-7
event messages
description, 2-5
format, 2-9
protocol entities, 2-6
severity levels, 2-6
exceptions, trap
configuring, 3-28
deleting, 3-30
EZ-Install, configuring BootP for use with, 4-13

F

forwarding mode (BootP), setting for router, 4-7
forwarding route, BootP
configuring, 4-9
disabling, 4-12
frame relay PVC, configuring BootP for AN router, 4-13

H

Hops parameter (BootP/DHCP relay agent interface), 4-5, A-16
host name of target BootP/DHCP server, configuring, 4-16

I

implementation notes, SNMP, 2-5
Input IP Address parameter (BootP/DHCP address), 4-11, A-19
Interface Priority parameter (BootP/DHCP relay agent interface), A-17
IP address
acquiring through BootP, 2-18
acquiring through DHCP, 2-14, 2-18
DHCP client, checking availability of address for, 6-4
DHCP server, specifying for, 6-2
NetID Server Manager, specifying for, 6-2
relay agent (BootP or DHCP), specifying for, 4-15
target server, specifying for, 4-15
IP Address parameter
BootP/DHCP client interface address, 4-14, A-21
IP configuration, 1-4
IP, starting, 1-2

L

lease requests (DHCP), specifying maximum number of pending, 6-6
Local IP Address parameter (DHCP server), 6-3, A-27
lock mechanism, SNMP, 3-4
Lock TimeOut parameter (SNMP global), 3-7, A-4

M

managers, SNMP
adding, 3-13
deleting, 3-17
description, 2-2
traps, configuring to receive, 3-14
Max. No. Pending Leases parameter (DHCP server), 6-7, A-26
memory use, for configuring thresholds, 2-10

N

NetID Management Console, 1-8

NetID Server Manager
description, 2-16
DHCP server port number, specifying, 6-3
IP address for communication with DHCP server, specifying, 6-2
port number, specifying for DHCP server, 6-3
requirement for DHCP server, 1-8
Number of Pings parameter (DHCP server), 6-5, A-25

O

operating mode, configuring for DHCP server, 6-5
Output IP Address parameter (BootP/DHCP address), 4-11, A-19

P

packets
BootP, 2-10
DHCP, 2-19
parameters, Site Manager, A-1
Pass Through Mode parameter
BootP/DHCP forwarding interface, 5-3, A-20
BootP/DHCP preferred server, 4-18, 5-3, A-23
BootP/DHCP relay agent interface, 4-6, 5-4, A-17
Ping Timeout parameter (DHCP server), 6-5, A-25
ping timeout value, specifying for DHCP server, 6-4
Polling Interval parameter (SNMP threshold global), 3-32, A-9
preferred server, configuring
BootP, 4-15
DHCP, 5-3
product support, xix
publications, hard copy, xviii

R

read/write access, restricting on SNMP router, 1-5
Relay Agent IP Address parameter (BootP/DHCP preferred server), 4-15, A-22
relay agent, BootP
customizing, 4-2
description, 2-11
forwarding table, specifying interfaces for, 4-9
passing packets to DHCP servers, 2-20
route forwarding, BootP
configuring, 4-9
disabling, 4-12

S

Safe Mode parameter (DHCP server), 6-6, A-26
Server Manager IP Address parameter (DHCP server), 6-2, A-24
severity levels, events, 2-6
show snmp commands, B-1
Simple Network Management Protocol. *See* SNMP
Site Manager paramaters, A-1
SNMP
agents, 2-2
applications, 2-2
authentication failure traps, enabling/disabling, 3-7
communities. *See* communities, SNMP
customizing, 3-1
description, 2-2
disabling, 3-3
enabling, 1-5, 3-3
event messages, specifying severity level for, 3-35
exceptions, trap
configuring, 3-28
deleting, 3-30
lock mechanism
disabling, 3-4
enabling, 3-4
specifying address, 3-6
specifying timeout value, 3-6
managers
adding, 3-13
configuring to receive traps, 3-14
deleting, 3-17
description, 2-2
messages, 2-2
Nortel Network-specific implementation, 2-5
proprietary implementation, 2-5
reenabling, 3-3
show commands, B-1
starting, 1-5
thresholds. *See* thresholds, SNMP
traps. *See* traps, SNMP

SNMP *(continued)*
type of service for packets, specifying, 3-9
view-based access control. *See* access control, SNMP view-based
starting
BootP, 1-6
BootP/DHCP relay, 1-7
DHCP server, 1-8
IP, 1-2
SNMP, 1-5
Subnet Mask parameter (IP configuration), 1-4
support, Nortel Networks, xix

T

Target Name parameter (BootP/DHCP preferred server), 4-16, A-23
Target Server IP Address parameter (BootP/DHCP preferred server), 4-15, A-22
technical publications, xviii
technical support, xix
text conventions, xvi
The, B-2
Threshold Action parameter (SNMP threshold interface), 3-37, A-13
Threshold Enable parameter (SNMP threshold interface), 3-34, A-9
Threshold High Event Level parameter (SNMP threshold interface), 3-36, A-12
Threshold High Value parameter (SNMP threshold interface), 3-35, A-12
Threshold HoldDown Intervals parameter (SNMP threshold interface), 3-39, A-14
Threshold Label parameter (SNMP threshold interface), 2-9, 3-39, A-15
Threshold Low Event Level parameter (SNMP threshold interface), 3-36, A-10
Threshold Low Value parameter (SNMP threshold interface), 3-35, A-10
Threshold Max Successive Alarms parameter (SNMP threshold interface), 3-38, A-14
Threshold Medium Event Level parameter (SNMP threshold interface), 3-36, A-11
Threshold Medium Value parameter (SNMP threshold interface), 3-35, A-11
Threshold Units parameter (SNMP threshold interface), 3-36, A-13
thresholds, SNMP
adding, 3-33
configuring, 3-31
description, 2-7
disabling, 3-31
enabling, 3-31
for a variable, 3-33
level, specifying, 3-34
memory considerations, 2-10
object name in an event message, specifying, 3-39
polling interval for a variable, specifying, 3-32
polling interval for held variables, specifying, 3-38
setting polling interval, 3-32
severity levels, 2-8
severity levels, events, 2-6
unit for a variable, specifying, 3-36
when to record events, specifying, 3-37
Timeout Secs. parameter (BootP/DHCP relay agent interface), 4-6, A-17
timeout, ping (DHCP server), 6-4
Transmit Bcast Addr parameter (IP configuration), 1-4
Trap Port parameter (SNMP manager), 3-15, A-6
Trap Types parameter (SNMP manager), 3-17, A-6
traps, SNMP
authentication failure, enabling/disabling, 3-7
configuring, 3-25
configuring a manager to receive, 3-14
deleting exceptions, 3-30
description, 2-2, 2-5
disabling an entity, 3-27
exceptions, configuring, 3-28
format, 2-7
severity level, specifying, 3-26
type, specifying, 3-16

U

UDP port number, 3-14

UnNumbered Assoc Address parameter (IP configuration), 1-4

unnumbered interfaces, for BootP and DHCP services, 4-15

Use Lock parameter (SNMP global), 3-5, A-3

User Datagram Protocol (UDP), 2-5, 3-14

V

views, SNMP access control. *See* access control, SNMP view-based

W

wildcards, using to configure SNMP views, 3-20